Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

1993

Monitoring technology proliferation: an open source methodology for generating proliferation intelligence

Green, Daniel M.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/39686

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

AD-A277 295

NAVAL POSTGRADUATE SCHOOL
Monterey, California

(2)

DTIC
ELECTE
MAR 2 8 1994
S F D

94-09399

THESIS

MONITORING TECHNOLOGY PROLIFERATION:
An Open Source Methodology for
Generating Proliferation Intelligence

by

Daniel M. Green

December, 1993

Thesis Advisor: Robert E. Looney

Approved for public release; distribution is unlimited.

94 3 25 086

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1993.	Master's Thesis December 1993

4. TITLE AND SUBTITLE MONITORING TECHNOLOGY PROLIFERATION: An Open Source Methodology for Generating Proliferation Intelligence

5. FUNDING NUMBERS

6. AUTHOR(S) Daniel M. Green

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(maximum 200 words)*

This thesis develops a methodology to monitor technology proliferation. It is designed to provide proliferation intelligence on specific threat technologies and can be used to augment export controls or enhance counter proliferation initiatives. A high-tech component used to upgrade underwater mines is the subject of the case study developed in this thesis. This technology monitoring method exploits the exponentially expanding volume of open source information occurring as a result of the information revolution.

14. SUBJECT TERMS

Technology proliferation, proliferation intelligence, technology monitoring, export controls, open source intelligence, mine warfare technologies, economic intelligence, economic security, underwater mines.

15. NUMBER OF PAGES
108

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01 280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited.

Monitoring Technology Proliferation: An Open Source Methodology for Generating Proliferation Intelligence

by

Daniel M. Green
Lieutenant, United States Navy
B.A., Villanova University

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

from the

NAVAL POSTGRADUATE SCHOOL
December 1993

Author: [redacted]
Daniel M. Green

Approved by: [redacted]
Robert E. Looney, Thesis Advisor

[redacted]
Edward J. Laurance, Second Reader

[redacted]
Thomas Bruneau, Chairman
Department of National Security Affairs

ABSTRACT

This thesis develops a methodology to monitor technology proliferation. It is designed to provide proliferation intelligence on specific threat technologies and can be used to augment export controls or enhance counter proliferation initiatives. A high-tech component used to upgrade underwater mines is the subject of the case study developed in this thesis. This technology monitoring method exploits the exponentially expanding volume of open source information occurring as a result of the information revolution.

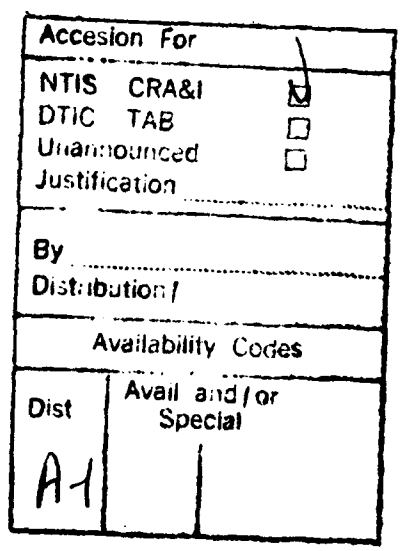

TABLE OF CONTENTS

I. TECHNOLOGY PROLIFERATION 1

A. INTRODUCTION 1

B. NATURE OF THE TECHNOLOGY PROLIFERATION THREAT 2

1. The Impact of the Geopolitical Revolution on Technology Proliferation 3

a. Export Controls: An Effective Cold War Regime 4

b. The Obsolescence of Export Controls 5

2. The Military-Technological Revolution 7

3. Evolution of the Global Economy 12

C. DOMESTIC CONSTRAINTS ON POLICY 13

D. MONITORING VS CONTROL AS A POLICY OPTION 14

E. A NEW APPROACH TO TECHNOLOGY MONITORING 18

F. SUMMARY 20

II. MODELING PROLIFERATION MARKETS 21

A. INTRODUCTION 21

B. THE NATURE OF PROLIFERATION 23

1. A Business Perspective on Proliferation 24

2. The Mechanics of Proliferation 27

C. THEORY 28

D. MARKET MODEL 30

1. Explanation of the Model 31

2. Levels of Analysis 33

E. STAGES OF THE PROLIFERATION PROCESS 34

F. FOREIGN MARKET ENTRY STRATEGIES 37

G. PHYSICAL DISTRIBUTION SYSTEM 40

H. CONCEPT OF CONTROL AND DEPENDENCY 43

I. SUMMARY 44

III. SOURCES AND COLLECTION TECHNIQUES 45

A. INTRODUCTION 45

B. OPEN SOURCES 46

1. Historic Uses of Open Sources 47

2. The Nature of Open Sources 49

C. COMMERCIAL COMPUTERIZED DATABASES 51

1. Database 51

2. Computers 53

3. Commercial 55

D. LIMITATIONS OF COMMERCIAL COMPUTERIZED DATABASES 56

E. TECHNIQUES TO EXPLOIT COMMERCIAL COMPUTERIZED DATABASES 59

1. Searching: An Iterative Process 60

2. When Can You Stop? 66

F. SUMMARY 67

IV. CASE STUDY 68

A. INTRODUCTION 68

B. MINE WARFARE: AN APPROPRIATE CASE STUDY 69

C. OVERVIEW OF MINE WARFARE 72

D. MINES AND THE MILITARY-TECHNOLOGICAL REVOLUTION 74

E. CUSTOMIZING THE TDD PROLIFERATION MARKET MODEL 76

1. The Mine Market 77

2. TDD Market 81

F. SUMMARY 83

V. CONCLUSIONS 85

A. IMPLICATIONS 85

1. Implications of Proliferation Markets 86

2. Implication of the Use of Open Sources 89

B. TOPICS FOR FUTURE RESEARCH 90

VI. BIBLIOGRAPHY 92

INITIAL DISTRIBUTION LIST 96

EXECUTIVE SUMMARY

The threat posed by technology proliferation did not end with the Cold War. In fact, the potential dangers associated with the globalization of military technologies are heightened by an ongoing military-technological revolution. Geostrategic changes and domestic economic constraints severely diminish the usefulness of traditional methods of countering technology proliferation (i.e., export controls). A new method is required, therefore, to monitor technology in order to provide some warning of technology's potential misuse.

It is no longer valid to view technology proliferation as a byproduct of military and ideological conflict. Proliferation in the post-Cold War environment is largely a function of dynamic interactions between corporate actors participating in highly competitive technology markets. By synthesizing aspects of several international business theories, this thesis develops a market model based on the legal, commercial aspects of technology proliferation. This model provides a visual representation of the technology proliferation process and provide a framework for proliferation intelligence efforts.

During the Cold War, open sources proved to be of limited use. Today, however, open sources can substantially augment traditional assets to monitor technology proliferation. Commercial computerized databases, because of their orientation toward business and industry, are open sources ideally suited to the investigation of technology proliferation markets. Since technology proliferation is largely a commercial exercise, techniques to exploit the capabilities of computerized databases can be borrowed from those used by corporate market analysts.

It is impractical to monitor the proliferation patterns of every technology. Analysts must concentrate on "threat technologies," i.e., those technologies that directly challenge the superiority of existing military weapons and systems. This thesis uses a minewarfare case study to demonstrate the technology monitoring method. Mines are a low cost, conventional deterrent that may prove decisive to the outcome of limited regional or littoral warfare. The ability to upgrade existing warstock mines to microprocessor controlled, multiple sensor, "smart weapon" systems significantly alters the calculus used to plan certain military operations. The degree to which these upgrade kits pose a threat can be evaluated by investigating the market for these Target Detection Device (TDD) upgrade kits. This case study reflects the first iteration of an investigation of the TDD market.

The technology monitoring method developed in this thesis can respond to requests for proliferation intelligence across the spectrum of warfare; from dual use technologies associated with weapons of mass destruction (WMD), to commercial or military technologies associated with the most mundane warfare subspecialty. A small team of analysts using this method and afforded adequate time, financial support, and the appropriate level of "command" interest, can provide unique intelligence support for policy makers and operational military commanders.

I. TECHNOLOGY PROLIFERATION

> We will give proliferation a higher profile in our intelligence collection, analysis, and defense planning and ensure that our own force structure and military planning address the potential threat from ... around the world.
>
> White House Press Release
> 27 September 1993

A. INTRODUCTION

Technology proliferation poses a potential national security threat to the United States because it undermines the technological superiority of U.S. military forces. In the past, this threat was addressed through the implementation of multilateral export controls. In light of recent geopolitical, economic and technological changes, however, the utility of export controls is increasingly being called into question. President Clinton recently stated:

> [F]or some time the United States has imposed stringent export controls on many of our most competitive exports .... One reason I ran for President was to tailor export controls to the realities of the post Cold War world.[1]

This section investigates the nature of the threat posed by technology proliferation, explains the changes that are leading to the obsolescence of export controls, and recommends a new method of monitoring technology to augment export controls.

---

[1]Quoted in Secretary of Commerce Ronald H. Brown, "Toward a National Export Strategy: U.S. Exports = U.S. Jobs," Trade Promotion Coordination Council, p. 54, 30 September 1993.

B. NATURE OF THE TECHNOLOGY PROLIFERATION THREAT

Technological superiority is one of eight principles supporting the National Military Strategy of the United States. It allows the United States to offset the quantitative disadvantage created by force reductions with a qualitative "high-tech" edge.[2] Superiority is a relative concept that depends not only on possessing and maintaining sophisticated weapons, but on preventing a potential adversary from obtaining qualitatively comparable systems.

The global proliferation of technology can increase the military capabilities of an adversary and undermine this strategy. Technology is defined by the Department of Commerce as "knowledge." This knowledge is first developed into a product or process[3] then incorporated into a military system, increasing the system's military capabilities. These improved capabilities, combined with intentions to challenge U.S. interests, constitute a discernable national security threat.

This threat is composed of three main components: potentially dangerous technologies, potentially dangerous users, and potentially dangerous proliferation patterns. To address this threat effectively, policy makers must know several things. First, they must know which technologies can be used to upgrade military systems. Second, they must know who among high risk technology users have

---

[2]Powell, Gen. Colin, National Military Strategy of the United States, 1993, p. 10.

[3]Technology is "embodied" in the product or process.

hostile intentions toward the United States. Third, decision makers must understand how technologies proliferate. Answering these questions, the what, who, and how of technology proliferation, is complicated by several interrelated trends: the geopolitical revolution stemming from the end of the Cold War; the military technological revolution; and the continuing evolution of the global economy.

1. The Impact of the Geopolitical Revolution on Technology Proliferation

The threat posed by technology proliferation was addressed during the Cold War largely through the implementation of export controls. The problem was simplified by the fact that the intentions of communist countries were assumed to be hostile. The solution, therefore, was straightforward: prevent communist countries from obtaining the capabilities provided by advanced technology.[4]

Since most countries of the industrialized West produced exportable technology, the effectiveness of national controls was largely dependent on the export policies of other nations. This problem was addressed at the international level by the Coordinating Committee for Multilateral Export Controls (COCOM).[5]

---

[4]Inman, B. R. and Burton, D. F., Jr., "Technology and U.S. National Security," p. 122, Rethinking America's Security, Allison and Treverton ed., W.W. Norton and Company, New York, 1992.

[5] While the Missile Technology Control Regime (MTCR) addresses some specific aspects of technology control, COCOM is the only international nonproliferation regime designed strictly for

As its name implies, COCOM coordinated the policies of individual member states to restrict the export of sensitive items which "... could contribute significantly to military potential and the proliferation of weapon systems, creating instability and international tension."[6]

COCOM developed three lists relating to military, nuclear and dual use technologies and products. Items on the lists were prevented from going to "proscribed destinations," the majority of which were communist countries. While the list of technologies evolved over the years, the regime reflected the static reality of a bi-polar international environment.

a. Export Controls: An Effective Cold War Regime

COCOM was an effective regime for several reasons. First, during the Cold War, international relations were dominated by military and ideological conflict between the socialist/communist East and the democratic/capitalist West. The clear and mutual threat to the industrialized nations during this East/West conflict encouraged cooperation and facilitated consensus on complex issues such as trade. Secondly, fundamental differences between free market economies of the West and centrally controlled economies of the East created natural barriers to trade: inconvertible currencies; lack of a legal framework for property rights

---

technology. COCOM members are the United States, NATO allies, Japan and Australia.

[6]Center for Non-Proliferation Studies, Inventory of International Non-Proliferation Organizations and Regimes. p. 18, June 1993.

and dispute resolution; and an inadequate banking system.[7] Communist markets could be written off by western entrepreneurs because commercial technology consumers existed almost exclusively in the West. There was little to gain from not engaging in multilateral controls and potential financial benefits that could be accrued from violating the export control regime were generally not worth the political risks. Finally, multilateral controls were successful because, until recently, the rest of the world was technologically dependent on the nations of COCOM.

b. The Obsolescence of Export Controls

The collapse of the Soviet Union, and the global forces which it unleashed, altered all of the conditions upon which multilateral export controls were based. The threat is no longer mutual or clear, free market capitalism is becoming the universal economic system, and convergence has destroyed the technological monopoly that the West previously possessed.

International relations are no longer dominated by military confrontation but by economic competition. The cost/benefit calculus of export controls has changed in light of threats posed by slow economic growth, negative

[7] The extent to which these differences created a barrier to trade is only now being fully realized as former communist countries attempt to develop free market economies of their own. See Blanchard, et al., Reform in Eastern Europe, United Nations University, 1992, for a comprehensive overview.

trade balances and industrial base vulnerability.[8] America's military allies are simultaneously economic rivals pursuing national or regional policies of economic expansion which are increasingly based on the development and export of high technology.[9]

The collapse of communism has left free market capitalism the dominant economic model. The restructuring that is occurring in previously controlled economies will break down the barriers formed by non-compatible economic systems creating lucrative, and competitive, new markets for high-tech products. Reducing export controls is viewed as mutually advantageous, helping the former communist countries develop while stimulating the economies of the industrialized nations. For example, the COCOM Cooperation Forum was established in 1992 in order to conduct the "progressive relaxation and elimination of export restrictions" on most formerly proscribed countries.

A waning desire on the part of the western industrialized nations to engage in broad, coordinated export controls coincides with the decreasing physical ability to enforce them. The combined efforts of Western nations are no longer enough to control technology because traditional sources are being joined

---

[8]Wallerstein, Mitchell B., "Controlling Dual-Use Technologies in the New World Order," Issues In Science and Technology, pp. 70-77, Summer 1991.

[9]It is true that this competition did exist in the Cold War, particularly in its latter stages. The disappearance of the Soviet threat, however, has removed almost all of the remaining national security dimension associated with broad export controls.

by other technology producers and suppliers. A greater and greater number of "Third World" nations, aided largely by western based multinational corporations (MNCs), are disregarding linear economic development theories and "leapfrogging" from pre-industrial societies to ones with dynamic high-tech segments. Brazil, India, and China are following this dualistic development strategy. Even poor countries, such as Indonesia, are investing billions of dollars into advanced technology industries in the hopes of emulating the economic success of the "Asian tigers."[10]

2. The Military-Technological Revolution

Admiral David Jeremiah, Vice Chairman of the Joint Chief of Staff, notes that technology is advancing at "breathtaking speed" across a broad spectrum of disciplines including robotics, biotechnology, artificial intelligence, directed energy weapons, and super-miniaturization. The development of defense applications for these advances could, he believes, cause "changes equal to those brought about by gunpowder or the internal combustion engine."[11] This Military Technological Revolution will alter existing concepts of war and profoundly affect the way it is waged in the future. While the benchmark for high-tech combat is

---

[10]The "Asian tigers" are South Korea, Singapore, Hong Kong and Taiwan. Shenon, Philip, "Indonesia Improves Life For Many But the Political Shadows Remain." The New York Times, p. A-1, 27 August 1993.

[11]Jeremiah, ADM David, "The Military and the Four Technological Revolutions," Defense Issues, Vol 8 No 5, p. 1, February 16, 1993.

currently Operation Desert Storm, a breakthrough in technology could result in the bulk obsolescence of weapons and systems employed during that conflict.

In the past, policy makers could count on the United States leading the world in technology development and applications, but this assumption is no longer valid.[12] New applications for both existing and emerging technologies are as likely to come from Southeast Asia as the "West" and, because of the changing nature of technology, may posses latent military capabilities that are not immediately recognizable.

Technology, more specifically high technology,[13] can be categorized as one of three types: military, commercial or dual use. Dual use technology has both military and commercial applications. The former Deputy Director of Central Intelligence, Admiral Bobby Ray Inman, points out that it is "increasingly difficult to separate civilian from military technology."[14] During the 1950's and 60's, technological breakthroughs came predominantly from defense related research and development. Technologies became dual use as commercial applications were developed or "spun off" from government R&D. Radar and jet engines, for example, were direct spinoffs from military R&D conducted at the

---

[12]Nelson, Richard R. and Wright, Gavin, "The Rise and Fall of American Technological Leadership: The Postwar Era in Historical Perspective," Journal of Economic Literature, Vol XXX, December, 1992.

[13]The Department of Commerce defines high technology as products having higher ratios of R&D expenditures to shipments than other product groups.

[14]Inman and Burton, p. 118.

end of WWII. During the past 20 years, however, cutting-edge technology has largely originated in the commercial sector, with dual use applications being "spun on" to the military sector. Current advances in computers and cellular telephone technology[15] are examples of continuing technology spin on. This phenomenon has tended to integrate the commercial and military technology sectors, increasing the number of dual use technologies and making military technological superiority largely dependent on commercial technological success.[16]

The nature of modern military systems contribute to this integration. Along with weapons, military systems increasingly include force multipliers which rely heavily on dual use technologies. For example, superiority in command, control, communications, and intelligence systems (C^4I) is intimately linked to developments in the rapidly changing telecommunications industry. It is rumored that Somali warlord General Aidid was able to evade UN forces by using a make-shift command and control structure based on cellular telephones.

A good illustration of how the dual use nature of technology complicates policy is reflected in the treatment of "critical tech. ologies." A perceived dependence on foreign industry for economic and military security

---

[15]Munro, Neil, "Pentagon Braces for New High-Technology Threats," Defense News, p. 3, September 6-12, 1993.

[16]Alic, John, et al, Beyond Spinoff: Military and Commercial Technologies in a Changing World, Harvard Business School Press. pp. 7-11, Boston, 1992.

prompted the U.S. Government to identify technologies vital to the U.S. national interest. These were termed "critical technologies." The National Critical Technologies Panel[17] developed a list of technologies that should "move into development and commercialization if the United States is to remain a world economic force."[18] The Department of Defense, as required by law, developed its own list, defining it as "technologies most critical to ensuring long term qualitative superiority of United States weapons systems."[19] The DoD list is compared to the NCTP list in Table I. The comparison clearly illustrates the policy dilemma faced by decision makers. Because they can be used for civilian and military purposes, technologies commercialized for economic gain must, at the same time, be controlled for military security.

---

[17] "The NCTP was appointed by the Director, Office of Science and Technology Policy (OSTP) and is required by the '90-'91 Defense Authorization Act to biennially report on critical technologies ... to increase government and industry awareness of the crucial role of technology in achieving national goals."
U. S. General Accounting Office, Foreign Technology: Federal Processes for Collection and Dissemination, Report No. GAO/NSIAD- Government Printing Office, p. 1, Washington, D.C. 1992.

[18] Rep. Tim Valentine, "Critical Technology: OSTP Report," Congress, House, Committee on Science Space and Technology, Subcommittee on Technology and Competitiveness, 102nd Cong., 1st sess., 25 April 1991.

[19] Department of Defense Critical Technologies Plan, ES-2, 15 March, 1991.

MILITARY POWER: TO BE CONTROLLED	**ECONOMIC POWER:** TO BE COMMERCIALIZED
DEPARTMENT OF DEFENSE	**NATIONAL CRITICAL TECHNOLOGIES PANEL**
1. Composite Materials	- Composites - Ceramics
2. Computational Fluid Dynamics	- Flexible Computer Integrated Manufacturing
3. Data Fusion	- Data Storage & Peripherals - Systems Management Technologies
4. Passive Sensors	- Sensors and Signal Processing
5. Photonics	- Electronic and Photonic Materials
6. Semiconductor Materials and Microelectronic Circuits	- Micro and Nano-Fabrication - Composites - Electronic and Photonic Materials - Micro and Opto Electronics - Material Synthesis and Processing
7. Signal Processing	- Sensors and Signal Processing
8. Software Producibility	- Software
9. Air Breathing Propulsion	- Aeronautics
10. Machine Intel/Robotics	- Intelligent Processing Equipment - Flexible Computer Integrated Manufacturing
11. Parallel Computer Architecture	- High Performance Computing and Networking
12. Sensitive Radars	- Sensors and Signal Processing
13. Signature Control	- Composites
14. Simulation and Modeling	- Computer Simulation and Modeling
15. Weapons System Environment	- High Definition Imaging/Displays
16. Biotechnology Materials and Processes	- Applied and Molecular Biology - Medical Technology - Pollution Minimization, Remediation and Waste Management
17. High Energy/Density Materials	- Composites - Ceramics
18. Hypervelocity Projectiles	- High Performance Metals and Alloys
19. Pulsed Power	- Energy Technologies
20. Superconductivity	- Surface Transportation Technologies - Energy Technologies

TABLE I. CRITICAL TECHNOLOGIES LISTS (Sources: DoD Critical Technologies Plan 1991, and OSTP Report on Critical Technologies, 1991.)

3. Evolution of the Global Economy

A recent National Academy of Engineers report highlights two "mutually reinforcing trends" that have, over the past twenty years, facilitated the development the global economy: technological convergence among the industrialized nations and the integration of "formerly discrete" national industries.[20] Corporations, responding to the new business challenges and opportunities posed by this global convergence and integration, are engaging in various activities that have changed the ways, the scope and the pace of technology proliferation. While international trade has substantially increased over the past several decades, export is only one of the ways that technology can be transferred. There are many corporate activities including the offset conditions related to foreign sales, that also contribute to proliferation.

In the process of responding to this changed environment, the structure of the corporation itself has evolved. The rise of MNCs, or the emerging Global Technical Enterprise, indicates that governments are joined on the world stage by new semi-autonomous actors. In a security environment based on economic competition,[21] governments will increasingly find themselves dependent on these international industries to accomplish national goals. Because, as "good corporate

---

[20]National Academy of Engineers, National Interests in an Age of Global Technology, p. 1, National Academy Press, Washington D.C. 1991.

[21]Bergsten, Fred C., "The World Economy After the Cold War," Foreign Affairs, p. 97, Summer 1990.

citizens," loyalties must be shared, corporate practices designed to exploit international markets may conflict with the desires of individual host governments. Governments are still able to regulate, facilitate, and substantially influence local operations, but they are finding it increasingly difficult to control global operations.[22]

C. DOMESTIC CONSTRAINTS ON POLICY

Initiatives to enhance national industrial competitiveness through the commercialization of high technology are taking precedence over those designed to counter potential military threats. For example, the Clinton administration recently removed national security export controls on a number of dual use computers and telecommunications technologies. Secretary of Commerce Ronald Brown stated that "80 percent of requests for export control licenses" were associated with these technologies.[23]

Any policy that advocates even the limited use of export controls is apt to be viewed as a double edged sword, hurting the initiator as much as dissuading the target country. The recent controls imposed against China, for sales of

---

[22] "Given a technological system that is truly international, national governments have lost much of their ability to control events through investments in technology or restrictions in its spread."
Alic, John A., et al., Beyond Spinoff: Military and Commercial Technologies in a Changing World, p. 12, Harvard Business School Press, Boston Mass., 1992.

[23] Interview between Ronald Brown, Secretary of Commerce and commentator on CNN program "Moneyline," 29 September 1993.

ballistic missile technology to Pakistan, are a case in point. They are estimated to cost U.S. exporters half a billion dollars in lost revenue.[24] Since they are unilateral actions, they do not prevent China from receiving the sanctioned goods from other sources.

The threat posed by technology proliferation is a function of the effectiveness of export controls. Since these controls are weakening, a method must be found to augment them. Policy alternatives, however, are constrained by a conservative fiscal environment. Declining budgets and political pressure generated by large fiscal deficits dictate that any new alternative be conducted by "forces in being" and not with new systems or bureaucracies.

D. MONITORING VS CONTROL AS A POLICY OPTION

Proliferation monitoring involves studying technology markets to identify the principle actors and activities associated with specific technology flows. The intelligence generated through the analysis of these markets can be used in conjunction with other methods of Indications and Warnings (I&W) to predict or prepare for future crises. Monitoring proliferation is well suited to a military security environment characterized by "instability" and nebulous threats because of the flexibility of the process. Resources used for technology monitoring can be oriented to specific technologies or actors and reoriented in a very short time.

---

[24]Greenhouse, Steven, "One Billion in Sales of High-Tech Items to China Blocked," The New York Times, p. A-1, 26 August 1993.

Monitoring is a reasonable addition to export controls because it addresses the threat while satisfying new economic constraints on policy. It requires no consensus among nations, special laws, treaties or agreements, and when open sources are used, it does not require procurement of new hardware or software systems.

There are many technology tracking/monitoring initiatives currently being pursued by the government. A 1990 U.S. GAO report found that six federal Departments and agencies account for the majority of federal technology monitoring efforts.[25] While a great deal of information is being collected, there are several obstacles hindering the effective dissemination and use of this information. First, interagency efforts are not coordinated. Second, technology databases contain both military classified and corporate proprietary information that preclude access to a wide variety of potential users. Third, hardware and software incompatibilities hinder the transfer of information even among "cleared" users.

These deficiencies are so severe that "the foreign technology information available from federal clearinghouses is generally neither current nor specific

[25]The Departments of Commerce, Defense, Energy, and State, the National Aeronautics and Space Administration (NASA) and the National Science Foundation.

enough to meet the needs of policy makers or industry representatives."[26] Government and industry officials prefer to rely instead on "private sector efforts ... because they are more focused on the needs of the their clients."[27] Private efforts through firms such as Technology Strategic Planning Inc., however, do have one major drawback: they are expensive.[28]

There are approximately thirty international non-government organizations (INGOs) and regimes concerned with proliferation issues. While they provide valuable worldwide coverage of many technologies, these regimes require the voluntary cooperation of signatories and are not universally adhered to.[29] The utility of these nonproliferation organizations and regimes is limited in several other ways as well. First, existing nonproliferation methodologies focus primarily on weapons of mass destruction (WMD) and their delivery systems.[30] Advanced conventional weapons and their associated technologies are not fully integrated

---

[26]U.S. General Accounting Office, Foreign Technology: U.S. Monitoring and Dissemination of the Results of Foreign Research, Report No. GAO/NSIAD-90-117, p. 2, Government Printing Office, Washington D.C. 1990.

[27]U.S. General Accounting Office, Foreign Technology: Federal Processes for Collection and Dissemination," pp. 2-3, Report No. GAO/NSIAD-92- Government Printing Office, Washington D.C., 1992.

[28]IBID, p. 31.

[29]Center for Non-Proliferation Studies, Inventory of International Non-Proliferation Organizations and Regimes, June 1993.

[30]Of the 31 international organizations and regimes concerned with proliferation, two thirds deal with weapons of mass destruction.

into the nonproliferation agenda. A "*threshold*" exists, therefore, below which technology tracking does not occur. Technological superiority implies dominance at all levels and across all areas of warfare. In the limited, regional conflicts currently envisioned by U.S. military planners and policy makers, sophisticated weapon systems well below the WMD threshold may hold the key to victory or defeat.

Second, the sale or purchase of technologies relating WMD are highly regulated or outlawed by international treaty and agreement. Tracking efforts are geared to countering proliferation. They focus on individual governments as actors and emphasize the military aspect of dual use technologies. The preponderance of military technology proliferation, however, occurs as legitimate international business. A monitoring initiative that is based on corporate practices and maintains a business perspective can encompass both the commercial and military aspects of dual use technologies as well as incorporate commonly used corporate technology transfer strategies.

Finally, existing technology tracking initiatives require large amounts of time, money and manpower. They are designed to be comprehensive because they provide the raw data for an array of international analysts and policy makers. These costs can be reduced by focusing on specific high interest technologies. Some technologies are related to key components of military systems that significantly enhance the sophistication of the system. The

monitoring of these individual "threat technologies" might be possible by a single analyst.

E. A NEW APPROACH TO TECHNOLOGY MONITORING

An approach to technology monitoring that dips below the WMD threshold, incorporates the commercial aspects of military technology proliferation, and provides a useful tool for the individual analyst is necessary to fill the gaps existing in current techniques. This new monitoring method should incorporate several important characteristics.

First, the method must be responsive to tasking from the national, operational, or tactical levels of decision making. Technology proliferation poses a potential problem for every level of the national security establishment. The monitoring method, therefore, must be decentralized and flexible enough to support all echelons. Since technology "below the threshold" is ubiquitous, it is impossible to track it all. Only previously evaluated and prioritized "threat technologies" will be monitored.

Second, the technology monitoring method must include a organized framework upon which the research can build. By viewing technology proliferation as a system, i.e., a collection of interdependent elements, a generic system model can be designed. This model, along with a reproducible procedure to allow customization of the model, provides the "guts" of the method.

Third, because they are not optimized for proliferation intelligence, traditional intelligence sources must be augmented through the exploitation of open sources. Monitoring technology proliferation is a multi-disciplinary activity which requires access to a wide variety of information. Open sources are uniquely designed to provide this access. One open source, computerized commercial databases, is particularly well suited to this role.

Fourth, the technology monitoring method must develop a technique to collect information from these commercial computerized databases. Since these databases contain such a great volume of information, means designed to extract only pertinent data must be developed. The business world, specifically in the field of competitive intelligence, currently employs the most advanced database search techniques. Applicable business techniques will be adapted to this method and augmented as necessary by "inventing" new ones.

Finally, the technology proliferation monitoring method must facilitate analysis of the information collected in order to make it useful to policy makers. Analysis turns information into intelligence. By providing a visual representation of the technology proliferation market structure, the method makes it easier to identify the vulnerabilities of the actors and activities engaged in proliferation. This intelligence will highlight political, economic and/or military options that may be applied in order to influence the system.

F. SUMMARY

The threat posed by technology proliferation did not end with the Cold War. In fact, the potential dangers associated with the globalization of military technologies are heightened by an ongoing military-technological revolution. Geostrategic changes and domestic economic constraints largely invalidate the usefulness of traditional methods of countering proliferation (i.e., export controls). A new method is required, therefore, to monitor technology in order to provide some warning of technology's potential misuse.

The remainder of this paper will be devoted to developing a new method for monitoring technology proliferation. First, the theoretical foundations of the method will be described. Proliferation markets will be explained and the framework, sources, and techniques needed to engage in monitoring will be identified. Next, the utility of the method will be tested by monitoring a specific technology. Finally, conclusions will be drawn regarding the process and its potential applicability to technology proliferation in general.

II. MODELING PROLIFERATION MARKETS

> The day is past when a major power can control the actions of small and regional powers through withholding defense material or technology. There is always a supplier who will step in to fill the vacuum...
>
> International Program Managers Handbook 1985.

A. INTRODUCTION

The West's collective Cold-War policy of communist "containment" included substantial provisions[31] for countering technology proliferation. Today, however, technology proliferation (or technology diffusion), is increasingly viewed as a desirable commercial activity that is essential to ensuring both national economic security and international stability. This philosophy is reflected in two policy initiatives recently announced by the Clinton administration: a foreign policy of "enlargement,"[32] and the supporting economic initiative of export promotion.[33] Other technology producers are adopting similar policies of export promotion.[34]

---

[31]Multilateral export controls under the COCOM regime.

[32]Friedman, Thomas L., "Clinton's Security Aid Gives A Vision of Foreign Policy," The New York Times, p. A-18, 22 September 1993.

[33]Brown, Ronald H., "Toward a National Security Export Strategy," Trade Promotion Coordinating Committee Report to the U.S. Congress, September 30, 1993.

[34]See Defense News, 6-12 September, 1993 for a number of articles concerning the commercialization of military and dual use technologies.

Section one discussed the potential threat posed by technology proliferation and explained the need for a new method to monitor this threat. Section two develops the foundations of a technology monitoring method that takes into account recent policy decisions. This new method addresses proliferation from a commercial perspective and explores the practical, business aspects of participation in international technology markets. By using this approach, decision makers will understand exactly how specific, potentially threatening technologies proliferate. An appreciation of the proliferation process will help officials to make informed decisions related to countering the proliferation threat.

To understand the proliferation process, a simple visual representation of the process is needed. This visual representation (the "Big Picture") is achieved by modeling the commercial aspects of proliferation, i.e., proliferation markets. The proliferation market model establishes a foundation for proliferation intelligence by providing a framework for information collection and analysis. The proliferation market model is superior to a proliferation data base because it allows bits of relevant information to be organized and displayed in a logical, interrelated format rather than simply as a list of disassociated data.

The accuracy of this market model is dependent on the validity of the theories from which it was developed. It is based on a synthesis of several economic theories heretofore not applied to the problem of proliferation: Michael

Porter's "Value System,"[35] Franklin Root's international trade theories,[36] and the logistics management theories of Magee, Copacino, and Rosenfeld.[37]

B. THE NATURE OF PROLIFERATION

Those who study proliferation have traditionally dealt with the exchange of Weapons of Mass Destruction (WMD) and associated technologies between state actors. One motivation for these governments to proliferate WMD sprang from military security and foreign policy concerns framed in terms of the East/West conflict. This nation-state perspective affects how the problem of proliferation is conceived: this state-centric view underlies the current "proliferation paradigm." For example, one assumption underlying this paradigm is that governments control the physical transfer of technology as part of their foreign policy. In other words, proliferation occurs as a direct result of calculated decisions by national governments. While this assumption was valid during the Cold War and remains largely true for weapons of mass destruction, it is increasingly invalid for military and dual use technology (including WMD technology).

---

[35]Porter, Michael, The Competitive Advantage of Nations, The Free Press, 1990.

[36]Root, Franklin, "Entering International Markets," Handbook of International Business, Chapter 31. Walter and Murray ed., John Wiley and Sons, 1982.

[37]Magee, John F., Copacino, William C., and Rosenfeld, Donald B., Modern Logistics Management: Integrating Marketing, Manufacturing and Physical Distribution, John Wiley and Sons, N.Y., 1985.

Now that the Cold War is over, government motivations concerning technology proliferation are becoming related increasingly to economic development and expansion. For instance, states are now more interested in promoting not controlling high-tech trade. Competitiveness in high technology markets has become synonymous with economic growth and prosperity in both the developed and developing world. As historic enemies move toward the development and integration of market economies, national governments will no longer desire or be able to control the infusion and diffusion of technologies in their countries.

With the demise of the Soviet Union came the end of the ideological, political, economic and military justification for many U.S. export controls. In this new environment, governments will be largely peripheral to the proliferation process. Technology proliferation will occur as a natural consequence of industrialization and modernization. Since threats to national security posed by technology proliferation are more nebulous than they were during the Cold War, it is necessary to investigate the nature of technology proliferation.

1. A Business Perspective on Proliferation

The revolutionary and evolutionary changes that have occurred in the global environment require that proliferation be analyzed at the corporate level. Investigation at this level-of-analysis ensures that proliferation variables associated

with dual use technologies, multinational corporations (MNCs),[38] and technology threats below the Weapons of Mass Destruction threshold are taken into account. For instance, dual use technologies proliferate not only between governmental sources and users in different countries, but also between multinational corporations and other non-government entities operating within the same state. Business strategies designed to make operations globally competitive also spawn subtle types of technology proliferation that are invisible at the nation-state level of analysis. For example, because of economic sanctions preventing foreign investment in South Africa, U.S. owned MNCs desiring to do business there resorted to (legal) company-to-company licensing and distribution agreements to maintain some foothold in the market. These agreements grew by over 300 percent over the past six years.[39]

Corporations are not conspiring against any particular government to create national security vulnerabilities. Most technology proliferation is legal and increasingly necessary for national economic health. At worst, corporations, especially MNCs, are oblivious to the national security concerns of host nations. They rely on the nations themselves to identify practices that are inimical to

---

[38]Corporations involved in international marketing production and physical distribution activities through export, licensing, joint venture, and fully owned subsidiary activities are referred to as multinational corporations. Magee, Copacino, and Rosenfeld, p. 200.

[39]Levy, Clifford J., "A Wary Reply To South Africa's Call," The New York Times, p. C-1, 21 October 1993.

national security. At best, corporations believe that their operations are inherently good, from a national perspective, bolstering national security by providing the economic and industrial base critical to the development of a robust military capability.

Currently the Clinton administration is attempting to forge post-Cold War strategies by dovetailing a foreign policy of "enlargement"[40] with an economic initiative based on export promotion.[41] These policies encourage both the opening and infusion of high technology goods into new markets, especially those of the former USSR and Eastern Europe. The execution of these policies will enhance the importance and influence of corporate actors.

The burden of determining which technology markets may pose a potential threat to national security is a responsibility that multinational corporations neither want nor can perform. As the influence and importance of corporate actors increase, government must be especially sensitive to indications of a market changing from "benign" to "malignant."[42] These indications are more likely to be identified in a timely manner if the mechanics of proliferation are

---

[40]Friedman, Thomas L.,"Clinton's Security Aid Gives A Vision of Foreign Policy," The New York Times, p. A-18, 22 September 1993.

[41]Bradsher, Keith, "U.S. Plans More Aid to Exports", The New York Times, p. C-1, 30 September 1993.

[42]The most clear cut case of a benign market becoming malignant is in the case of Iraq where a militarily aggressive regime used computers transferred via legitimate trade to develop a nuclear weapons program. This has become the prototypical situation for threat technology proliferation.

thoroughly understood. A less than healthy appreciation of how proliferation occurs may lead to the improper evaluation of potential threats and the development of inadequate policy options to counter those threats.

2. The Mechanics of Proliferation

Technology proliferation results from interactions between the market forces of supply and demand. Demand is created by a technology user attempting to satisfy its own needs or desires for a product. Technology sources monitor their markets, identify and/or stimulate these demands, and then attempt to satisfy the demand by supplying the desired technology product.

Technology proliferation occurs when actors develop strategies and perform activities designed to allow technology to flow from one place to another. It is comprised of two distinct activities: (1) technology transfer and (2) physical transfer of goods. The Department of Commerce defines technology transfer as:

> The transfer of knowledge generated and developed in one place to another, where it is used to achieve some practical end.[43]

Physical transfer is usually viewed in terms of the export/import trade of technology products. The two types of transfer that make up proliferation are distinct. They can occur independently or concurrently depending on the type of agreements negotiated between actors. Both, therefore, must be incorporated into a monitoring method if it is to be comprehensive.

---

[43]U.S. Department of Commerce, Office of Administration, Lexicon of Trade Terms, 1992.

C. THEORY

As previously stated, technology poses a potential threat when high technology products are used to upgrade or enhance a weapon or military system. The degree to which these new capabilities constitute a threat can be assessed by investigating the international markets for these high-tech products.

An international market is defined as "a group that has similar patterns of need, purchasing behavior and product use."[44] Corporations that choose to conduct business internationally pursue strategies that allow them to become or remain competitive in selected markets. Competitive means, very simply, that the benefits of market participation exceed the costs. Benefits include showing profit, gaining market share in a particular product, or gaining access to foreign markets for a variety of products. Cost relates to expenses for such things as labor, materials and overhead that are required during a manufacturing process. Risk is the dynamic that changes the cost/benefit calculation. For example, the risk associated with business investments in Russia is considered high in light of recent unrest there. Corporations develop marketing strategies designed to increase benefits, limit costs and, most importantly, minimize risk.

In practice, because international markets are so complex, in depth market analysis is used to develop successful strategies. Market analysis is an executive

---

[44]Davis, Stanley, "Organization Design," Handbook of International Business, Walter and Murray ed., Chapt 39 p. 14, John Wiley and Sons, N.Y., 1982.

decision support tool that allows corporations to compare the sum of market participation costs to the sum of the benefits. Additionally, it incorporates the risk factors associated with market participation that change this cost/benefit calculus.

Corporations attempt to analyze and understand markets in order to compete within them; they must investigate all internal and external aspects of the market. Susan Douglas and Samual Craig list 38 decision variables that should be evaluated with regard to cost, benefit and risk prior to market entry. They are grouped under five major headings: financial, technical and engineering feasibility, marketing, economic and legal, political and social.[45]

This study of proliferation markets maintains a corporate perspective but ultimately has non-corporate objectives. It determines how proliferation markets work to identify policy options that will allow external leverage to be exerted on the market. Therefore, markets do not have to be evaluated from a cost, benefit, and risk perspective, but from the standpoint of market vulnerabilities such as single sources, foreign dependency, and logistics bottlenecks. Limiting the number of variables greatly simplifies both the nature and scope of the market analysis needed.

---

[45]Douglas, Susan P., and Craig, C. Samual, "Information for International Marketing Decisions," Handbook of International Business, Chapt 29 p. 14, Walter and Murray, ed., John Wiley and Sons N.Y. 1982.

Economist Michael Porter proposes that the best way to understand markets is to view them as a "value system: the entire array of activities involved in a product's creation and use."[46] In other words, to understand a product market sufficiently enough to be competitive (business) or to wield influence (government), the entire process (the supply of raw materials, manufacturing, distribution channels and sales to the ultimate user) must be evaluated as an "interdependent system or network of activities."[47] This mutual dependence means that each element affects the efficiency of the system. Efforts to influence the system are enhanced by knowing the specific elements of the market. In the case of a proliferation market that has turned malignant, each element can be reviewed to determine what combination of leveraging options (political suasion, diplomatic negotiations, economic sanctions, or military strikes) can be applied to the system to disrupt the undesirable flow of the technology product.

D. MARKET MODEL

Corporate actors, industrial activities, business strategies and distribution flows or channels are elements common to the value systems of all technology markets. A model can be used to represent these generic aspects of the system.

---

[46]Porter, p. 579.

[47]This statement relates to Porter's concept of the value chain which he defines as "an interdependent system or network of activities connected by linkages. Linkages occur when the way in which one activity is performed affects the cost or effectiveness of other activities." Porter, p. 41.

A model organizes the system into logical relationships between elements and provides a simple visual representation of the complex interactions generally engaged in by market participants.

The remainder of this section is a step by step examination of the underlying assumptions, generalizations, and logic used to develop the generic technology proliferation market model shown in Figure 1. The objective of the model is to provide the reader with a simple yet representative display of the proliferation market system.

1. Explanation of the Model

This is a model of the value system for a generic manufactured hi-tech product. Suppliers provide physical and technology inputs to a source where they are combined by manufacture into a product. The source develops a strategy for breaking the product into foreign markets, transferring some combination of physical product and/or technology across an international border to an ultimate user.

Flow diagram symbols are used to represent the actors, activities, strategies and flows of the market. Actors, represented as ovals, are the companies or corporations that execute the proliferation process. The activities, represented by rectangles, are the types of business practices that the actors must conduct in order for proliferation to occur. These activities can be broadly grouped into two categories: pnysical transfer and technology transfer. Strategies, the rounded squares, are the ways that actors develop foreign markets for their

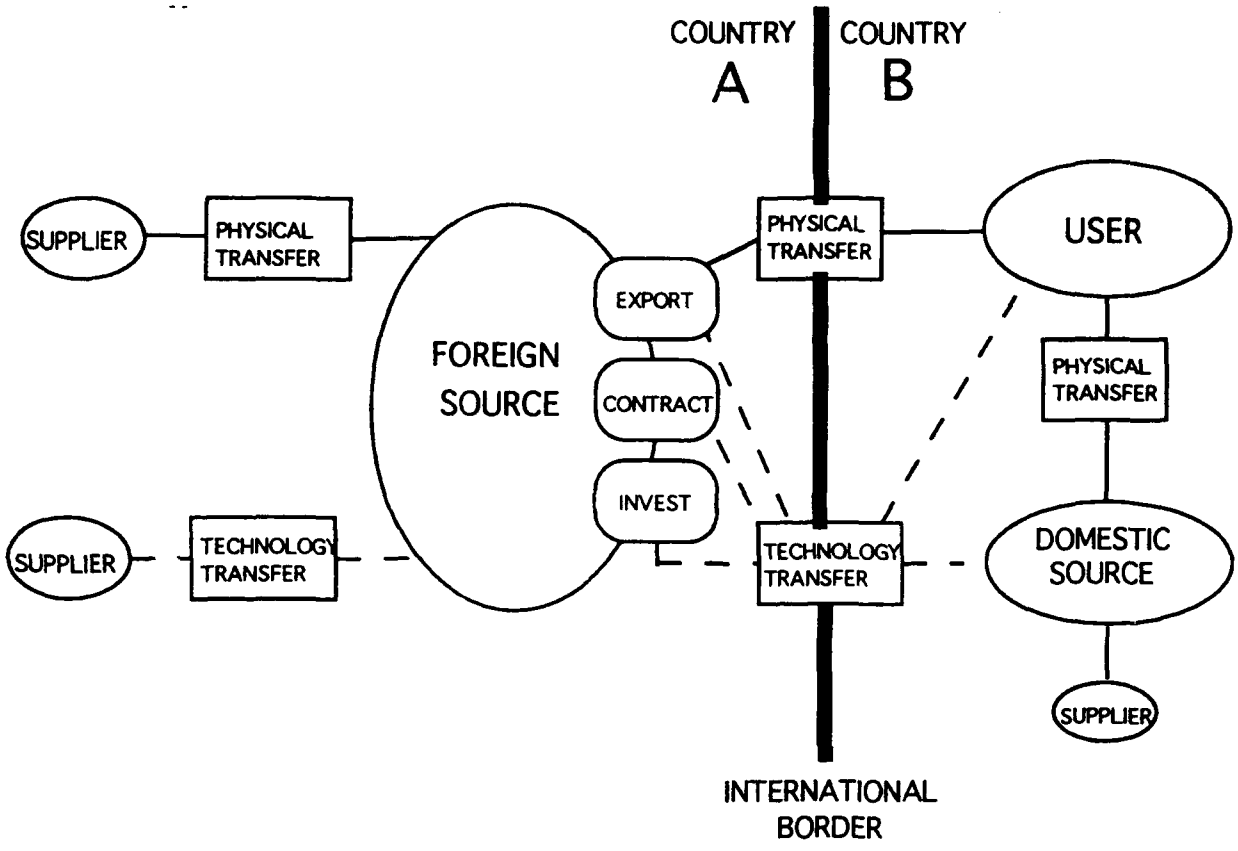

Figure1: GENERIC PROLIFERATION MARKET MODEL

product, including exporting, contracting, and investment.[48] The distribution flows, or channels, link the elements together and are represented by the lines connecting actors to activities. Solid lines represent physical product flows and dashed lines indicate technology flows.

2. Levels of Analysis

This model functions at three different levels of analysis: actors, activities and product of the market. As discussed earlier, this proliferation monitoring method will investigate corporate actors and industrial activities relating to specific technology products.

A technology product can be viewed at various levels of aggregation depending on the stage of the manufacturing process: raw materials, components, or systems. At the component level, the product is at a high enough level of

Table II Levels Of Analysis

	NATION-STATE
ACTORS -----	**CORPORATIONS**
	INDIVIDUALS
	BUREAUCRATIC
ACTIVITIES --	**INDUSTRIAL**
	INDIVIDUAL

[48]Root, pp. 31.4-31.5.

aggregation to allow tracking but still low enough to reflect dual use characteristics. Components have a narrow range of applications in contrast to raw materials that have a range of applications that make tracking nearly impossible. Components used to upgrade or enhance military systems are likely to have dual, or multiple uses. As the level of technology aggregation increases into the system level, however, applications become more specific, clarifying the distinction between military and commercial use. If technologies are all tracked at the system level, therefore, some components with military applications will not be monitored because they are part of a commercial system.

Table III Product Level of Analysis

HIGH	**SYSTEM**
Level of Technology Aggregation	**PRODUCT --- COMPONENT**
	RAW MATERIAL
LOW	

E. STAGES OF THE PROLIFERATION PROCESS

The model represents four stages of technology proliferation: (1) pre-manufacturing, (2) domestic source manufacturing, (3) foreign source manufacturing, (4) and post-manufacturing. During the product pre-manufacturing stage, the source receives inputs of materials and technology from suppliers. Materials can be raw (plastics, metals, ceramics) or semi-manufactured, for example microelectronic computer chips. These materials must be transferred

by physical means such as plane, rail, truck or ship. Technology inputs are the research, development, design and/or fabrication of a product. The Department of Commerce notes that technical "knowledge" may be:

> transferred by giving it away (technical journals, conferences, emigration of technical experts, technical assistance programs), industrial espionage, sale (patents, blueprints, industrial process) or the activities of multinational corporations.[49]

Technology transfer is more difficult to track than physical transfer because of technology's ethereal nature. Blueprints, for example, can be faxed, transferred in a briefcase or in someone's brain. Technology transfer is not impossible to track, however, because it is, to a large extent, subject to international business laws and norms.[50]

During the manufacturing stage, a source combines materials with technology to form a product. When both the manufacturer and the user reside within the same state, a product is described by the model as originating from a domestic manufacturing source.[51] No technology proliferation occurs in the case of totally indigenous production, (i.e., where all materials, technology, manufacturing, and use occur in the same country). In practice, however, many

---

[49]Department of Commerce, Lexicon of Trade Terms.

[50]Intellectual or industrial property rights.

[51]The terms domestic and foreign relate to the technology user.

domestic manufacturing capabilities are dependent on foreign technology especially those in the newly industrializing nations.[52]

In domestic manufacturing, foreign companies often serve as technology suppliers, transferring this technology in accordance with a variety of business agreements. Michael Broska and Thomas Ohlson provide the following list of agreements that contribute to technology proliferation:

> Joint production, licensed production, subcontracting in the purchasing country for components and spare parts, transfer of research and development capabilities, marketing rights, maintenance contracts for regional users of the weapons systems, and imports of other industrial goods from the weapon recipient by the supplier country.[53]

These agreements, known as offsets, are becoming increasingly common as developing countries attempt to lessen their dependence on foreign technology and build an indigenous industrial base. While the term "offset" is most often associated with the globalization of defense industries, it is occurring across the technology spectrum.

Foreign source manufacturing occurs when the process of combining materials and technology into a product is performed in a country other than that

---

[52]Meier, Gerald, M., Leading Issues in International Development, Fifth Edition, pp. 268-273, Oxford University Press, 1989.

[53]Brzoska, Michael, and Ohlson, Thomas, Arms Transfers to the Third World, 1971-1985, p. 131, Oxford University Press, 1987.

of the ultimate user. The product must then be physically transferred during the post manufacturing stage via the export/import process.[54]

The fourth and final stage, post manufacturing, consists of marketing, selling, distributing and servicing the technology product.[55] These activities are combined in the model under the generic headings of "Physical" and "Technology Transfer." The model shows physical transfer and technology transfer as parallel proliferation activities because in practice they often occur simultaneously.

Physical transfer can be an extremely complicated evolution involving many secondary actors and activities. The field of logistics management evaluates the activities associated with physical transfer in terms of a physical distribution system. Technology transfer, an equally complex phenomenon, is a function of the strategies that corporations use to enter foreign markets.

F. FOREIGN MARKET ENTRY STRATEGIES

Expanding from domestic to foreign markets is a complicated but increasingly necessary corporate process.[56] The evolution of the global economy forces corporations to develop effective mechanisms to stretch their value chain,

---

[54] It is at this point in the process that governments have traditionally addressed technology proliferation by regulating exports and imports.

[55] Yip, George, Total Global Strategy: Managing for Worldwide Competitive Advantage, Prentice Hall, 1992.

[56] Taylor, Charles R., "Global Presence and Competitiveness of the U.S. Manufactures," Conference Board, New York, 1991.

a system of interdependent industrial activities,[57] across international borders. Firms enhance their international competitiveness by developing specific foreign market entry strategies. Franklin Root defines these foreign market entry (modes) strategies as:

> Institutional arrangements that enable a company to transfer its products, technology, management, and other resources to a foreign country.[58]

He places these strategies into three major categories: contractual, investment, and export. The proliferation market structure is delimited by the strategy selections of the corporate actors.

In a contractual strategy, technology is transferred from a source in one county to a source in a second country where actual manufacture takes place. The technology transferred, according to Root, is usually some form of "industrial property rights such as patents or individual know how."[59] Root also lists eight types of contractual strategies: licensing, franchising, technical agreements, service contracts, management contracts, construction or turn-key contracts, and co-production agreements.[60] Contractual strategies are less risky than direct foreign investment, which requires substantial capital outlays. Also, contractual strategies

---

[57]Porter, p. 41.

[58]Root, p. 31.4.

[59]Root, p. 31.12.

[60]Root, p. 31.4-31.5.

avoid both import tariffs and the licensing delays associated with an export strategy.

An investment strategy, like a contractual strategy, transfers technology from a source in one country to a source in a second country where manufacturing takes place. Corporations establish subsidiaries in different nations either through direct acquisition of a foreign firm, cold start up of a new company, or various joint ventures in which the multinational shares a percentage of the ownership with a host nation corporation. An investment strategy allows a corporation to exploit the competitive advantages of the host country to a greater degree than is possible through a contractual strategy.[61] Corporations engaging in investment strategies are likely to transfer industrial and intellectual property rights, as well as manufacturing and managerial know how.

The third foreign entry strategy, export, is also the most familiar to students of proliferation. Export strategies consist of physically transferring products across national boundaries. It can also include technology transfer such as that which occurs through an after-sales service contract. Service contracts not only include repair and replacement of parts but enhance the capability of a product through the transfer of technical "know how" or experience. The benefits of an export strategy depend to a great extent on the design of the distribution system that moves products between countries.

---

[61]Root, 31.16.

G. PHYSICAL DISTRIBUTION SYSTEM

Products that are exported or imported are physically transferred through the distribution system. This system incorporates all aspects of product transportation and storage. Time, distance, and space are vitally important aspects of the physical transfer process. Unlike the technology that is transferred in a licensing agreement, for example, products cannot be digitized and "faxed" to anywhere in the world instantaneously. Many variables including a products size, weight, and shape must be considered when determining the most cost effective mode of transportation. In turn, the way a product is transported determines the time it takes to get a product from source to user. Storage is also time and space dependent. Very few products are manufactured in lots of one. The output of production runs becomes inventory which must be stored at various locations before reaching the ultimate user. These warehouses or stock points (including weapons armories) are important because they affect the rate of technology proliferation.

Companies that wish to engage in an export strategy must coordinate the activities of a number of secondary actors such as banks, insurance companies, various governmental agencies (e.g., Customs and Commerce), shippers, and carriers.[62] Each of these actors has specific requirements that must be satisfied before product transfer occurs. Requirements can become so complex that many

[62]Magee, Copacino, and Rosenfeld, p. 195.

corporations rely on companies that specialize in facilitating the export/import process. Freight forwarders, for example, are involved in all aspects of planning and conducting the international shipment of goods from a product's source to its final destination. They help arrange for the most cost effective physical movement of exports as well as assist in completing important transportation documentation.[63] A general appreciation of the actors and activities of the physical distribution system will enable an analyst to tap into the flows of information that control and record the material movement of technology products.[64] Figure 2 depicts a generalized physical distribution subsystem.

Many of the critical nodes, consolidation points, and bottlenecks of the value system occur in the physical distribution system. By concentrating on these potential logistics vulnerabilities, analysts can determine specific points at which leverage can be applied to influence a malignant market. For instance, the time it takes to deliver a product from port A to port B provides a window of opportunity for interdiction. Secondary actors can provide information on the specifics of past shipments or serve as the focal point for economic sanctions or

---

[63]Functions include: cargo consolidation, booking space on ships, preparing export declarations, import permits, commercial invoices, consular invoices, bills of lading, certificates of origin, insurance, and collecting payments for shipments. Magee, Copacino, and Rosenfeld, p. 196.

[64]Magee, Copacino, and Rosenfeld, p. 2.

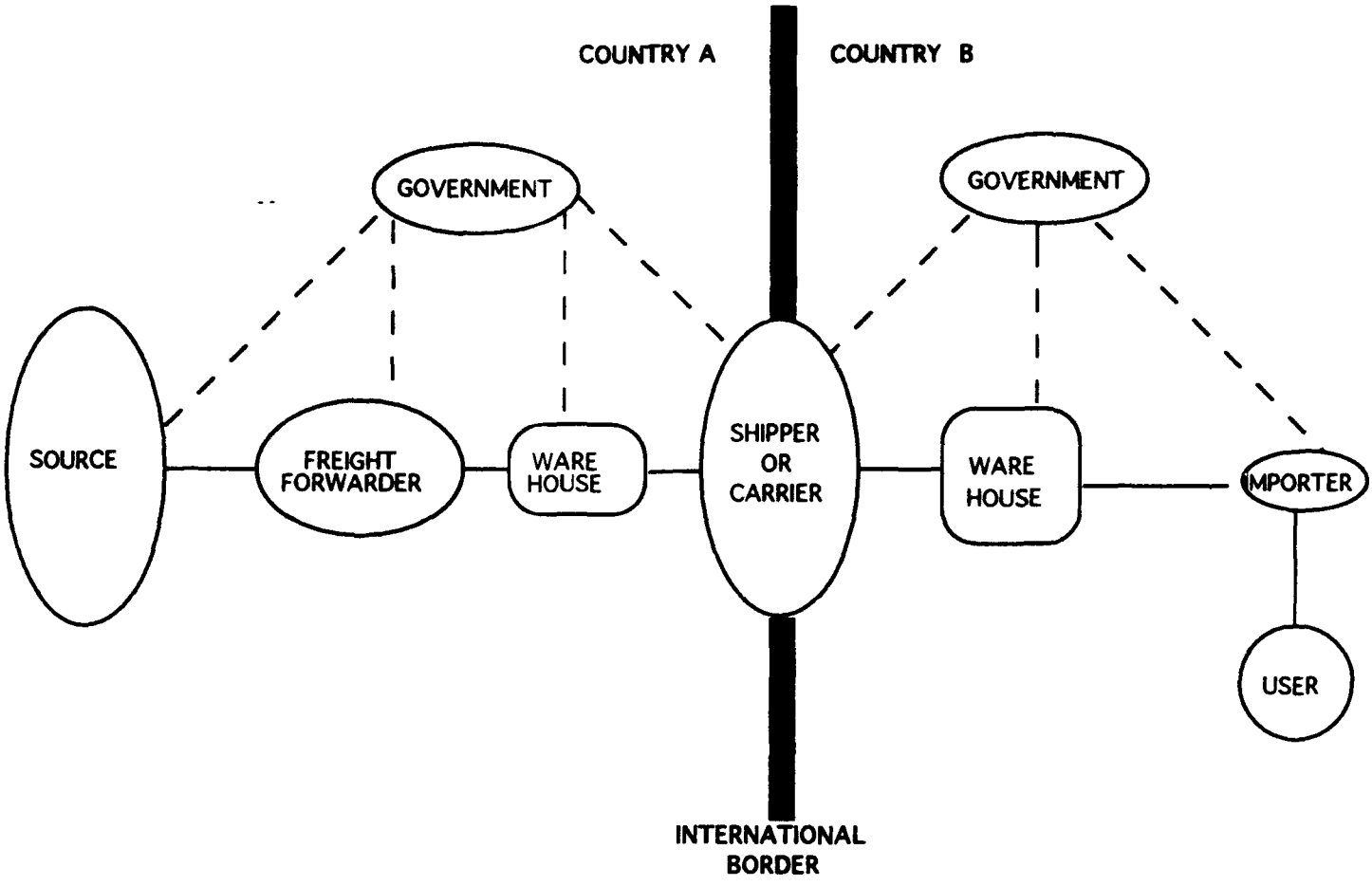

Figure 2: PHYSICAL DISTRIBUTION SYSTEM

diplomatic protest.[65] And, when military force is being considered as an option, warehouses represent prime targets.

H. CONCEPT OF CONTROL AND DEPENDENCY

System actors control the process of technology proliferation. The actors decide the type, quantity, quality, method, and timing of the proliferation process. As the number of actors increase, power is diffused, making the system more difficult to control internally and more complicated structurally. These actors have various degrees of control depending on their position within the system. The primary actors, USERs, manufacturing SOURCEs, and SUPPLIERs, are critical to system operation and therefore have the greatest influence. Secondary actors are associated with the physical distribution process. They are vital to the system but they depend on, and are constrained by, decisions of the primary actors. Tertiary actors are governments whose main function is regulation rather than control of the technology proliferation process. Governments react to decisions by the primary actors.[66]

---

[65]Companies as the focal point of diplomatic protest is not a new idea. Recently the U.S. government filed a protest with Thailand over the activities of one of its companies in Libya.

[66] In government owned industries or centrally controlled economies, governments function as primary actors.

I. SUMMARY

In light of the changing geostrategic landscape and recent U.S. initiatives, the process of technology proliferation must be reevaluated. It is no longer valid to view technology proliferation as a byproduct of military and ideological conflict. Proliferation in the post-Cold War environment is largely a function of dynamic interactions between corporate actors participating in highly competitive technology markets. By synthesizing aspects of several international business theories, a market model based on the legal, commercial aspects of technology proliferation can be developed. This model provides a visual representation of the technology proliferation process and provide a framework for proliferation intelligence efforts.

The next section investigates sources of information and collection techniques that are used in customizing the generic technology proliferation market model into a product specific one.

III. SOURCES AND COLLECTION TECHNIQUES

> The Intelligence Community's current challenge is to expand the use of open sources to cover a broader range of issues such as weapons proliferation, economic competitiveness and the environment.
>
> Admiral William Studemann
> Deputy Director of Central Intelligence[67]

A. INTRODUCTION

The economic questions raised in the analysis of technology proliferation markets cannot be answered merely through a realignment of the technical and human assets that served the intelligence community well in the past. New sources of information must be found and exploited. Decision makers need to develop an appreciation for the value of these new sources and analysts must be trained in effective collection techniques. This chapter describes open sources and explains how open source information can be applied to the problem of technology proliferation. One open source of information that is uniquely designed for the investigation of proliferation markets, commercial computerized databases, is examined in detail. Techniques to exploit this potential source of intelligence are also introduced.

---

[67]Studemann, Admiral William, "Teaching The Giant To Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community". Unpublished paper presented at the First International Symposium on National Security and National Competitiveness: Open Source Solutions, December 1992.

B. OPEN SOURCES

In an era of declining defense budgets, new sources of intelligence information must be both affordable and currently available. Requests for the development and acquisition of unique hardware systems or the procurement and integration of unproven software programs are unlikely to be greeted with much enthusiasm or funding. These fiscal constraints, however, may turn out to have the positive consequence of forcing a complete evaluation of the intelligence potential of open sources.

A leading proponent of using open sources for intelligence applications, Robert Steele, defines them as information sources that are "not classified at their origin, are not subject to proprietary constraints other than copyright, are not produced by sensitive contacts requiring obscuration and are not acquired through clandestine or covert means."[68] By definition, open sources contain neither classified military nor proprietary corporate information nor does their exploitation constitute industrial espionage. Open sources are particularly suited to an investigation of technology proliferation markets because international business is a relatively transparent endeavor compared to intelligence collection tasks of the past.

Bureaucratic inertia, the inability of large organizations to change rapidly enough to conform to contemporary requirements, may hinder acceptance of open

---

[68]Steele, Robert D., "Open Source Intelligence Clarifies Global Threats," Signal, September 1992.

sources as an intelligence tool on a par with classified sources and methods. Interestingly, this inertia may be more psychological than structural. The use of open sources requires a fundamentally different approach toward and attitude about the intelligence cycle[69] than is used when exploiting classified sources.

1. Historic Uses of Open Sources

Open sources were not used extensively in the past because of the nature of the Cold War threat. Hostile target nations were characterized by closed societies in which public and published data were controlled by centralized, totalitarian governments. These governments were supported by extensive internal security organizations whose modus operandi was disinformation, both for foreign and domestic consumption. The nature of these target countries lead to the development of collection strategies geared to uncovering their "secrets."[70] In this "data poor environment," large amounts of time, effort, and money were required to uncover small amounts of usable intelligence.

---

[69]The intelligence cycle is the process by which information is acquired, converted to finished intelligence and made available to policy makers. Richelson, Jeffry T., The U. S. Intelligence Community 2nd ed., p. 3, Harper Business, 1989.

[70]Admiral William Studemann, "Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community."

The need to maintain intelligence capabilities suited to a data poor environment has not disappeared.[71] However, most societies today are characterized by a combination of both open and closed segments. This is increasingly true of those countries which do not threaten the United States directly but retain the capability to do so, such as Russia and China. Therefore, in addition to the traditional intelligence sources and techniques used to collect secret information, open sources and techniques must be developed to allow threat analysis of the open aspects of adversarial societies.

When using open sources and techniques, the activities of the intelligence cycle[72] are conducted in a "data rich environment." The analysis problem in this type of collection environment consists of sorting through, and making sense of vast quantities of information in a timely manner. Disinformation is less likely because of the decreased desire and ability of a government to conduct a coordinated campaign. The problem of misinformation however, data that is partially or totally incorrect but not part of a planned coordinated strategy, still exists. An open source strategy must necessarily incorporate methods to mitigate this problem.[73]

---

[71]Countries such as North Korea and Iraq very much fit the closed country mold and remain the United States' most visible threats.

[72]Planning and direction, collection, processing , production and analysis, and dissemination. Richelson, p. 3.

[73]Such as by verification through multiple sourcing.

2. The Nature of Open Sources

The concept of exactly what constitutes an open source has changed dramatically over the past few years. As late as 1989, Jeffry Richelson, a noted author on intelligence organizations, described open sources as "newspapers, magazines, and unclassified journals as well as public radio and television."[74] His examples of open source applications highlight their severe limitations during the Cold War.[75] Just three years after Richelson's book was published, Admiral William Studemann, Deputy Director of Central Intelligence, presented a paper before the First International Symposium on National Security and National Competitiveness: Open Source Solutions in which he addressed the increasing utility of exploiting open sources to answer qualitatively new questions being posed to the intelligence community. He significantly expanded Richelson's definition to include "printed material such as books, magazines, and newspapers as well as maps, photographs, data files, digital imagery and broadcast media."[76]

The utility of open sources has been enhanced not only by recent geostrategic changes but by the evolution of information technology. Over the

---

[74]Richelson, p. 250.

[75]Open sources permitted the identification of Yuri Andropov as the person chosen to lead Brezhnev's funeral procession. Deductive analysis of that bit of data led Kremlinologists to predict that Andropov would follow Brezhnev as Soviet Chairman. Richelson, p. 253.

[76]Admiral William Studemann, "Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community."

past decade, advances in microelectronics have allowed greater and greater amounts of information to be stored in increasingly smaller physical space. Software developments facilitated the growth of the personal computer industry by making computers "user friendly." This encouraged the development of computer applications in disciplines other than the computing sciences.[77] The invention of supporting systems such as modems has allowed the rapid transmission of data over installed telephone lines. New hardware (e.g., text scanners) and processes (e.g., photocomposition) permit tremendous volumes of textual material, such as books, periodicals, and newspapers to be easily placed in computerized format. Digitization, storing information in binary code (i.e., on a laser disc) as opposed to storing information in electric fields (i.e., on magnetic tape), affects information storage, retrieval and transfer in ways which are just beginning to be realized. The planned replacement of current telephone lines with fiber optic cable will provide even greater impetus to the information revolution by allowing the transfer of text, sound, and images at the same time.[78] CD-ROM is the Model-T Ford of this multiple medium industry.

In the post Cold War world, the Intelligence Community is not responding to traditional country threats (e.g., USSR) but to a threat environment (e.g., weapons proliferation, general instability). Part of this threat environment

---

[77]Those based on mathematics and physics.

[78]See Ramirez, Anthony, "A War Within a Single Wire," The New York Times, p. C-1, 27 October 1993, for an indication of future practical applications of telecommunications technologies.

is characterized by an opening of societies, greater information flow, and new technologies that allow the exploitation of open sources in ways which were never before possible.

C. COMMERCIAL COMPUTERIZED DATABASES

The most promising open source for the study of proliferation markets is commercial computerized databases. The exploitation of these databases will not make technology tracking easy, but it will make monitoring possible. There remains a great deal of confusion and skepticism regarding the utility of commercial databases as an intelligence source and the applicability of computers to non-computing problems. It is therefore necessary to examine exactly what a commercial computerized database is, how it differs from other databases, what role the computer plays, and why this open source is useful in customizing proliferation market models.

1. Database

A database, very simply, is a means by which information is organized and stored. While databases can consist of many different types of information, for example words, numbers, images, and sounds,[79] it is the textual databases, those containing words, which are used in this current project. Although use of the term "database" implies "computerized," theoretically speaking, a database can

---

[79]Williams, Martha E., "The State of Databases Today: 1993" Gale Directory of Databases, p. xxi, Gale Research Inc. January 1993.

exist without a computer. A paper filing system is an example of an elementary "database." As used here, databases are filing systems that have evolved in the age of computers.

Databases can be maintained in two ways, locally or remotely. A local database is one in which the user collects, organizes, updates, and retrieves information according to its specific needs. A company's personnel files are an example of a local database. The contents of a local database are not limited, however, to internal information. External information, such as might be collected by a company's marketing division, can also be part of a local database. Because they control the entire process, users are more familiar with, and have greater confidence in, local databases. A remote database is one in which information collection, organization, and maintenance are performed by someone other than the user. The user, therefore, has no control over the contents of the database. The user gains access rights to the information contained in the remote database by contracting with a commercial supplier.[80]

One can begin to appreciate the volume of material contained in databases after citing some relevant statistics. Martha Williams notes that the number of databases has doubled in the past five years to over 7000. This

[80] There are remote databases that contain public information, such as those on the INTERNET, but their evaluation and use is beyond the scope of this report.

represents 4.527 billion database records each of which contains 200-2000 words. For comparison, this page of typed text contains just over 200 words.[81]

These statistics are impressive, but are only important if the databases provide information that facilitates the modeling of proliferation markets. In fact, the majority of databases do just that by providing a wealth of information on specific companies, the technology patents which they hold, their marketing strategies, and even data concerning contract negotiations.[82] Many other databases also have potential direct application. For instance, those containing bibliographic data and news stories allow the analysts to tap into information which has already undergone some preliminary analysis.

2. Computers

Computers enhance the use of databases by providing the physical means by which this vast amount of information can be manipulated. They do this in several ways. First, computers make databases easier to develop and maintain by permitting large amounts of data to be placed rapidly in common formats such as lists or files. Secondly, they allow this data to be arranged and rearranged in innumerable ways, permitting the creation of information products

---

[81]Tracking technology is only one application of database exploitation. Because databases are expanding exponentially and database search skills are not part of most analysts tool kit, an almost untapped source of potential intelligence information currently exists. This source and the skills necessary to exploit it constitute a new field: Database Intelligence (DBINT).

[82]Williams, p. xx

tailored to meet specific needs. Finally, and most importantly, computers permit a user to access rapidly and sort through the vast amount of information that databases provide.

It is important to understand what roles computers are not playing in this investigation of proliferation markets. Computers are not performing calculations. There are no algorithms (formulas) being used that allow questions to be posed, computations to be performed, and answers about the proliferation process to be derived. Neither are computers being used here in conjunction with Decision Support Systems (DSS). DSSs use artificial intelligence to assess and compare the variables of complex problems to determine the "best" course of action. While it is true that computers can and are being used by various intelligence agencies in the above modes to conduct multivariate trend and threat analysis, they are used in this project for data retrieval only.

In this application, information is stored on computers in databases that are remotely maintained. Access to this information is legally gained by contracting with a database company. Information is physically extracted or pulled from the database by using a password supplied by the company, a personal computer equipped with a modem, and a printer. The information thus retrieved constitutes raw data. The value of this data is not a function of computer hardware or software but is dependent on the skills and insight of the analyst. Computers, therefore, neither substitute for analysis nor displace the analyst. On the contrary, computers increase the need for systematic methods of

evaluating large quantities of very different types of information and put a premium on the skills and work of educated, and highly motivated, analysts.

3. Commercial

Commercial databases are particularly well suited for the investigation of proliferation markets for several reasons. First, commercial databases are geared toward business applications. Of the 7841 entries listed in the 1993 edition of Gale's Directory of Databases, 4116 (53 percent) relate to business, science, technology and engineering.[83] Second, databases are expanding in scope to provide potential information on global proliferation activities and actors. In fact, the only continent that is not specifically covered by a database is Antarctica.[84] Third, competition is forcing the database industry to respond to user demands, making databases more accessible to the general public.

Buying access to commercial databases is cost effective because of the amount of information that they contain. Since these databases are remotely maintained, the costs in manpower, time, and money associated with computer hardware, database development and maintenance[85] are borne by the database producer. Also, commercial databases fees are not based on constant rents but on the amount of time a user is actually looking for, retrieving or extracting

---

[83]Williams, p. xxv.

[84]Williams, p. xxiii.

[85]Updating a database to keep it comprehensive and current.

information.[86] This pay-as-you-go aspect is particularly attractive during a period of fiscal constraint.

Because there are over 7000 commercial databases, it is difficult to know which ones contain specific data applicable to a particular product market. Database vendors partially solve this problem by providing access to many databases at the same time. For example, for a minimal fee[87] the DIALOG vendor service allows access to over 450 databases. DIALOG recently entered into an agreement with a second vendor service, DATASTAR, which expands the available access to over 525 databases. DATASTAR is known for its comprehensive coverage of European corporations. DIALOG/DATASTAR was selected for this study because it is a currently existing source at both the Naval Postgraduate School and at various intelligence agencies of the U.S. government.

D. LIMITATIONS OF COMMERCIAL COMPUTERIZED DATABASES

The two greatest limitations associated with commercial computerized database exploitation are the inability to access fully all material referenced on certain databases and the fact that they are not all standardized in a "user friendly" format. The first limitation relates to the database entries themselves.

---

[86]The information on databases can be stored on magnetic tapes or compact discs (CD-ROM) and mailed to the user. This method has some cost advantages such as no online or download fees. However, the disadvantages are that the information may be old, only one database can be accessed at a time, and each database must be purchased separately.

[87]$295.00

Not all databases contain entire books, articles, or papers. Instead, they provide short abstracts of the information contained in these documents and a bibliographic reference as to where the articles can be found. Complete entries known as "full text," are becoming increasingly common and, undoubtedly, will someday be the standard.[88] Until then, an analyst must have access to a well stocked research library.

The second limitation relates to what is known in computer circles as the "user-interface." Many analysts and researchers who could potentially use these databases are either not aware of their existence or know that pertinent information exists but do not have the time, inclination or opportunity to learn how to use them.[89] Databases and the computers on which they are stored, are research tools and, like any tool, require a certain degree of skill to use. To effectively locate and retrieve information, a researcher must have some familiarity with a computer keyboard and an understanding of the fundamentals of word processing.[90] More importantly though, a researcher must develop a familiarity with the contents of the databases being exploited.

---

[88]Currently, full text is available on 50% of all commercial databases. Williams, p. xx.

[89]Based on an informal survey of professors at NPS.

[90]In fact, excessive preoccupation with developing computer competency tends to shift the focus of the analyst away from the potential of the information and toward the potential of the hardware.

Databases contain different types of data and often require slightly different methods of retrieval for each type of information. The database industry is attempting to standardize these retrieval methods, but is being hindered by the industry's explosive growth. Generally speaking, access is gained to the information in the database by conducting a series of steps on the computer keyboard known as access protocols. By conforming to these protocols, the researcher is speaking the database language and can therefore communicate specific requests for information. This skill requires an inquisitive attitude, and the ability to read and understand instructions related to general computer software commands. It is best honed with practice, but a great deal can be learned away from the computer through literature provided by commercial database companies and/or specialized magazines such as Database and Online.

This requirement for specific skills highlights a related limitation, the dependence on intermediaries. Most people with the skills necessary to exploit databases are not the people who fully understand the requirements and goals of the research being conducted. These intermediaries, in the form of research librarians and/or private companies specializing in information retrieval, currently serve as a necessary link between the information source and information user. They may also serve, however, as a buffer and unintentional filter through which information must pass. This filtering can dilute the utility of the information and the effective use of databases in general.

Currently, most analysts determine what to look for while intermediaries determine where and how to look for the information. It is helpful if the intermediary knows something about the subject under investigation, but this is not always possible. The analyst requesting specific information is, therefore, limited by his or her ability to explain the nature of the research to the intermediary and by the intermediary's knowledge, skill and motivation. The potential of commercial computerized databases as an intelligence source will not be realized until the researcher/analyst develops the necessary skills to displace intermediaries and thereby decrease the effects of filtering.

Even with these limitations, commercial computerized databases represent a unique collection environment that provides information well suited to the task at hand. The remainder of this section identifies techniques to retrieve information pertinent to proliferation markets. These techniques can be used directly by an analyst or can be explained to and performed by an intermediary.

E. TECHNIQUES TO EXPLOIT COMMERCIAL COMPUTERIZED DATABASES

The process of finding and retrieving information from databases is called "searching." The most important aspect of database exploitation is the development of a clear, concise search strategy. Effective strategies are critical to cost and time efficient use of databases. Search strategies consist of three parts:

identifying the pertinent type of data; identifying the data's location; and determining how to retrieve it.

To know exactly what information is needed, an analyst must have some expertise on the subject in question. This can be accomplished by consulting known "experts" or conducting substantive research prior to going "on line" (the term used to describe time actually spent connected to the database). This expertise helps define the precise key terms, or word combinations required for an effective search.

The second part of the search strategy is knowing where the greatest potential exists for finding the type of information being sought. Each search strategy will be somewhat unique, requiring access to different combinations of databases. This requires some familiarization with the content of the database.

The third part of the strategy involves certain techniques that affect how the information is retrieved. These techniques consist of a combination of keywords and search options provided by installed "correlation" software. Some techniques being developed by corporations to enhance their competitiveness in domestic and international markets can be adapted to the modeling of proliferation markets. These business techniques will be used in conjunction with the development of new techniques that fit the specific needs of the project.

1. Searching: An Iterative Process

Searching the computerized database for information to customize a specific proliferation market model is an iterative process. Initially, a general

search should be conducted to determine the amount (i.e., number of articles or "hits"), the kind (e.g., historical records, technical reports) and the location (i.e., which databases) of available information. Since the market model is product specific, an initial general search strategy would begin by determining the keywords and phrases associated with the selected product.

Search strategies require that requests for information be framed in terms of Boolean, AND/OR/NOT, logic. Boolean logic "translates" a research question into a format that the computer understands. Computers will only recognize combinations of terms already programmed into the database software. While seemingly simple, Boolean logic can be frustrating, especially for an analyst deeply involved in research. Very early on, a researcher internalizes basic assumptions regarding the research. These assumptions must be "explained" to the computer.

For example, the case study for this project was conducted by a naval officer searching for information on a specific electronic component associated with mines. A logical initial keyword, therefore, would be "mines." If this keyword was used, however, a great deal more information would be extracted than desired. For instance "mines" would retrieve database entries on gold mines, strip mining, and even black lung disease (disease, mine). This spurious information costs both money and time and is an example of the pitfalls of a faulty search strategy. Table IV displays some keyword combinations that would result in some spurious information.

Once the proper combination of keywords and phrases is discovered, synonyms must be investigated. As noted before, not all databases are standardized. Terms used to access the same type of data may vary slightly from database to database. For example, "mine parts" could be listed as "accessories," "components," or "upgrades." Table V lists some possible combinations of

KEYWORD	**SPURIOUS INFO**
MINES	GOLD MINES
MILITARY MINES	LAND MINES
UNDERWATER MINES	SEA BED MINING
NAVAL MINES	PARTIAL INFORMATION

TABLE IV: Keywords

"AND" Logic	Mines AND Naval	Mines AND Underwater	Mines AND Marine
"OR" Logic	Mines AND Sea OR Acoustic OR Pressure		
"NOT" Logic	Mines AND Naval NOT Land		

TABLE V: AND/OR/NOT Logic

keywords and phrases associated with the case study.

Fortunately, when dealing with manufactured products, there is a short cut in the use of Boolean logic. Manufactured products are grouped by industrial or "product codes." These codes are based one of three industrial classification systems: the Standard Industrial Classification (SIC),[91] Standard International Trade Classification (SITC), or Harmonized System (HS). SIC has traditionally been the most important because it is "the classification standard underlying all establishment based U.S. economic statistics classified by industry."[92]

SIC based product codes are two to seven digit numerical codes which indicate two things. The numbers themselves indicate different products in various industries. The amount of digits in the number indicates the degree of aggregation of the products within an industry. As the number of digits increase, the code indicates a much narrower range of products. An example of SIC based product codes is shown below.

The level of aggregation that a searcher chooses will depend on the product being investigated or the iteration of the search. When tracking specific technology products it is appropriate to use the greatest level of disaggregation; the seven digit product code. This level of aggregation is one or two levels above the optimum level for component tracking but does significantly reduce the volume of information that must be evaluated.

---

[91]Executive Office of the President, Standard Industrial Classification Manual 1987, Office of Management and Budget.

[92]Department of Commerce, Lexicon of Trade Terms.

SIC BASED PRODUCT CODES

SIC Code	Level	Description
20-39	Major Groups	Manufacturing
34	Major Group	Fabricated Metal Products
348	Industry Group	Ordnance and Accessories
3483	Industry	Ammunition, except for Small Arms
34833	Bombs, mines, torpedoes and parts	Product Class
3483316	Marine Mines and Parts	Product

TABLE VI: Standard Industrial Classification Codes

Because the codes are standardized, they always pertain to the same products. Fortunately product codes are one way in which many databases can be accessed. Finding and using the appropriate codes are the first steps to a successful search. SIC based product codes are listed in the Numerical List of Manufactured and Mineral Products published by the Bureau of Census and available through the U.S. Government Printing Office.

Of the two other codes used in industrial circles, SITC can be discounted because it does not go below the four digit level of disaggregation. Codes based on the Harmonized System, are used in the classification of international products. This system was partially adopted by the United States

on January 1st, 1989 and is adhered to by 50 other industrialized countries.[93] Harmonized codes are much different than the SIC based ones. Since both codes are used in various databases, both must be known. The Harmonized System codes for this project's case study are listed below.

HARMONIZED SYSTEM CODES
9306 Bombs, grenades, torpedoes, mines, missiles, and similar munitions of war and parts thereof....
9306.90.80.6 Parts for bombs, grenades, torpedoes, mines and similar munitions of war.

TABLE VII: Harmonized System Product Codes

Keeping in mind that information is being retrieved in relation to the proliferation model, a second search may focus on another element of the value system, such as the actors. Information should answer questions, such as where the source's factory is physically located and what is the manufacturing plant's production capacity. Is the company a multinational and if so, who are the company's foreign subsidiaries and parents? What patents does the company hold? What is the size of the companies export market? The information is inserted into the appropriate place in the model. As each new piece of

[93]Department of Commerce, Lexicon of Trade Terms.

information is added, the model is customized to represent the actual market structure.

2. When Can You Stop?

Each iteration of the search allows a more specific investigation of an element in the model. Theoretically, iterative searching could continue until the research budget was exhausted, the information was so specific that no further data existed in the databases, or the model was a perfect representation of the actual market. In practice however, the number of searches will be limited by funding and the specific requirements of the originator.

The investigation of proliferation markets will be conducted in response to specific requests for information from operators and/or policy makers. Strategic concerns may be answered in the first few iterations if, for example, the request is to correlate actors with the countries in which they operate. If the model is being used to address tactical concerns, such as the location of the warehouses in which a specific product is stored, many iterations will be needed. These searches may not provide information specific enough for decision making, but can significantly narrow the intelligence collection "field of view" so that classified sources can be employed. The importance and true utility of this method exists as an augmentation to more traditional forms of intelligence collection and analysis.

There is no way to determine if an analyst has extracted all the pertinent information relating to the market under investigation or how accurately

the model reflects the actual proliferation market structure. Success of the method is measured not in terms of how comprehensive the information is, but if, at the end of the evolution, more pertinent information exists than before.

F. SUMMARY

During the Cold War, open sources proved to be of limited use. Today, however, open sources can augment traditional assets and provide valuable intelligence data on some non-traditional threats facing the United States. Open sources are particularly useful for monitoring technology proliferation. Commercial computerized databases, because of their orientation toward business and industry, are open sources ideally suited to the investigation of technology proliferation markets. Since technology proliferation is largely a commercial exercise, techniques to exploit the capabilities of computerized databases can be borrowed from those used by corporate market analysts. The following section uses a case study to investigate the utility of the technology proliferation monitoring method.

IV. CASE STUDY

The task of defining threat technologies - be it the most sophisticated anti-ship missiles or the simplest of small arms and hand planted mines - is foremost."

Office of Naval Intelligence
Posture Statement, May 1993[94]

A. INTRODUCTION

Previous sections of this report identified the threat posed by technology proliferation, established a theoretical foundation for the investigation of technology proliferation markets and explained how to use open sources and techniques to gather proliferation market intelligence. This section uses a case study to illustrate the general utility of the technology proliferation monitoring method.

It is impractical to conduct an analysis of proliferation markets for every technology in every warfare area. Analysts must concentrate on high-tech products posing the most serious military threats. For the purpose of this report, high-tech components that can be used to enhance or upgrade the sophistication of a weapon or military system are termed "threat technologies." Threat technologies occur in every warfare area, from the "high end" to the "low end" of the military spectrum. For example, at the high end of the spectrum, near the weapons of mass destruction (WMD) threshold, the incorporation of satellite

[94]Sheaffer, Radm Edward D., Office of Naval Intelligence Posture Statement, May 1993.

based, commercially available, GPS (Global Positioning System) technology into a ballistic missile's inertial navigation system significantly enhances the accuracy of that weapon system. At the low end of the spectrum, the incorporation of microcomputers and advanced passive sensor technology into the firing circuits of naval mines have changed these devices from relatively simple to smart weapons. The mine component that serves as the "brain" for current generations of intelligent mines, the Target Detection Device (TDD), is the subject of this case study.

B. MINE WARFARE: AN APPROPRIATE CASE STUDY

Iraqi mining operations during the Gulf War raised concerns among civilian and military officials about the capabilities of U.S. mine warfare forces. During that conflict, mines severely damaged the USS Tripoli and USS Princeton. According to General Walter Boomer, Commanding General of the First Marine Expeditionary Force during Operation Desert Storm, underwater mines were also a major consideration in the decision not to attempt an amphibious landing on the Kuwaiti coast.[95] In light of these events, the Office of Naval Intelligence requested that research be conducted on the proliferation of technologies associated with mine warfare.[96] In response to this interest, this investigation

---

[95]"The Assault That Wasn't," Navy News and Undersea Technology, June 29, 1992.

[96]Unclassified internal memorandum from Office of Naval Intelligence to National Security Affairs Department, Naval Postgraduate School, April 1993.

provides a strategic assessment of regional underwater mine markets as well as tactical intelligence to support "pro-active" mine countermeasures. The Mine Warfare Plan defines pro-active countermeasures as efforts aimed at "preventing the enemy from laying mines against U.S. and allied naval forces by destroying the mines at points of manufacture, storage, depots or during transport."[97]

This case study also demonstrates the validity of the technology proliferation monitoring method developed in this report. Mine warfare clearly illustrates, in several respects, the changing nature of technology proliferation and the necessity of developing a fresh perspective on this potential threat. First, the United States does not maintain technological superiority in mines[98] and is only now, after several decades of fiscal neglect, capable of fielding mine countermeasures forces technologically comparable to its NATO allies.[99] U.S. mine inventories consist of weapons that currently lag several generations behind mines available on the international market. From a proliferation standpoint, since the United States does not produce or export current generation mines, national export controls

---

[97] Mine Warfare Plan, p. 39.

[98] While this mine inventory is not obsolete and the most sophisticated mines can be bought from NATO allies, the U. S. inventory will be severely depleted by the end of this decade. Foxwell, David, "Naval Mine Warfare: Unfunded and Underappreciated," p. 128, International Defense Review, Vol 2, 1993.

[99] MCM-1 Avenger class minesweepers and MHC-51 Osprey class mine hunters are outfitted with the world's most sophisticated mine countermeasures gear.

cannot be used to counter the spread of these weapons or their associated technologies. Even information about the size and scope of the market is difficult to obtain because the U.S. government is more likely to have information on a technology market in which U.S. companies are actively competing.[100]

Second, the reorientation of the U.S. National Military Strategy from global to regional conflict and the concurrent shift of U.S. naval doctrine from open ocean to littoral warfare[101] substantially increase the importance of amphibious and mine warfare in relation to other warfare areas. Mines are the weapon of choice for many developing countries and may, in a regional context, prove to be the ultimate conventional deterrent. John Mearsheimer defines conventional deterrence as "denying an aggressor his battlefield objectives with conventional forces."[102] A review of mining operations conducted since WWII[103] indicates that mines have been successful when used in this role.

Third, the military-technological revolution is affecting the development of mines in ways that highlight the reasons why technology proliferation well below the Weapons of Mass Destruction threshold cannot be ignored. While the

---

[100]The U.S. mine inventory consists principally of iron bombs converted into mines.

[101]United States Department of the Navy, ...From the Sea: Preparing the Naval Service for the 21st Century, Government Printing Office, September 1992.

[102]Mearsheimer, John, Conventional Deterrence, p. 15, Cornell University Press, 1983.

[103]Mine Warfare Plan, p. 18-24.

military-technological revolution is affecting both the mining and countermeasures aspects of mine warfare, the technology associated with mines is advancing more rapidly than mine countermeasures technology. Mine "counter countermeasures" such as intelligent hunter mines with "home on ping,"[104] severely complicate mine warfare operations and tactics.

Finally, while the weapons themselves do not have dual use applications, this is not true of the components used to upgrade them. Target Detection Devices (TDD) for instance, combine the latest microprocessing computer technology with advances in passive sensor technology.[105]

C. OVERVIEW OF MINE WARFARE

Mine warfare can be divided into two broad categories: mining and mine countermeasures (MCM). Mining encompasses all of the variables associated with placing an effective configuration of weapons in the water. Minefield location, geometry, weapons mix, and the best mine delivery method, must be determined. Mines can be used in accordance with an offensive or defensive strategy to deny access to harbors or coastal waters, to interrupt sea lines of communication (SLOCs), or to delay the seaborne operations of an adversary (e.g., amphibious assault). The United States conducted a successful offensive strategy during the

---

[104]"Mine Aimed at MCMV's," Jane's Defense Weekly, p. 95, May 26, 1990.

[105]Passive sensors are one of the critical technologies listed in chapter one p. 11.

Vietnam War when it mined Hiaphong Harbor and closed North Vietnam's most important port for 300 days.[106] Successful defensive mining operations were most recently used during Operation Desert Storm. Iraq sewed ten minefields, consisting of 1100-1300 weapons, along the coast of Iraq and Kuwait that interrupted the naval operations of coalition forces and helped to deter an amphibious assault.

There are two general types of mines that are designated in accordance with their method of actuation: contact or influence.[107] Contact mines are usually tethered, or moored, to the seabed by cables or chains. They are detonated when a vessel physically comes into contact with horns protruding from the mine body. Influence mines can be either moored or designed to rest on the sea floor (also known as ground mines). They sense the magnetic, acoustic, and/or pressure signatures of a ship as the vessel moves through the water. The most sophisticated influence mines use combinations of magnetic, acoustic, pressure, and even seismic sensors to enhance both the sensitivity of the mine and its ability to discriminate between targets.

The second major area of mine warfare is mine countermeasures (MCM). Mine countermeasures are designed to reduce the effectiveness of an adversaries

---

[106]Hartmann, Gregory, Weapons That Wait: Mine Warfare in the U.S. Navy, Naval Institute Press, 1979.

[107]Specialty mines such as CAPTOR and modern hunter mines are a combination of mines and torpedoes. These hybrids use influence sensors and can be considered an evolution of the ground mine.

mine forces by preemptively destroying mines prior to their deployment in the water, finding and marking minefields so they may be avoided, or detonating mines in a controlled manner through sweeping or hunting. Moored mines can be neutralized through mechanical sweeping methods. Mine sweeping vessels or helicopters tow "sleds" through known or suspected minefields. This mechanical sweep gear cuts the mooring cables causing the inherently buoyant mines to float to the surface where they can be destroyed by small arms fire. Some influence mines can also be swept. Devices that generate simulated magnetic and/or acoustic signatures cause mine detonation as they are towed or piloted through the water. Mine sweeping is the fastest way to clear a minefield but it is not effective against pressure actuated influence mines. These weapons must be hunted. Mine hunting consists of searching, detecting, and classifying mines so that they may be neutralized, one at a time, by divers or Remotely Operated Vehicles (ROV).[108]

D. MINES AND THE MILITARY-TECHNOLOGICAL REVOLUTION

Underwater mines and associated technology have traditionally been very slow both to develop and to become obsolete. Contact mine technology developed at the turn of the 20th century is still a viable threat on the eve of the

---

[108]Increasingly, remotely operated vehicles such as the U.S. Navy's mine neutralization system (MNS) are being used in both mine sweeping and hunting.
"Naval Mine Warfare Supplement," International Defense Review, p. 10, 11/1989.

21st.[109] The current weapon inventories of many Third World countries consist of mines produced shortly after World War II.[110] A review of the high-tech applications currently being incorporated into mines, however, indicates that mines are rapidly evolving into sophisticated weapon systems. Microprocessors, sonar systems, non-metallic construction materials, unique architectural designs, absorptive coatings, advanced sensors, anti-swimmer devices, remote actuation, and propulsion and guidance systems are being incorporated into the newest generations of mines.

A related technological development of particular concern to those decision makers responsible for evaluating specific regional threats, is the introduction of modular upgrade kits that can be reterofitted to existing mine warstocks. These kits replace a mine's firing circuits with modern electronics, turning relatively simple underwater ordnance into computer controlled, multiple sensor "smart" weapons.

The ability to retrofit existing warstock mines with a microprocessing "brain" has several major implications for mine and littoral warfare. First, force packages and strategies used to counter mines depend on the type, (bottom, moored), the actuation device, (magnetic, acoustic, pressure), and mix of mines. Second,

---

[109]In 1987 and 1988 respectively, the US flagged oil tanker Bridgeton and the USS Samual B. Roberts struck contact mines that were of pre-World War One design (Mk08).

[110]Jane's Undersea Warfare 1993-94, p. 170, Jane's Information Group Ltd. 1993.

external identification of the mine, required in mine hunting, is no longer a valid indicator of a mine's capabilities.[111] Even contact mines can be upgraded into multiple sensor devices. Third, the purchase of TDD upgrades invalidates known mine orders of battle.

These TDD upgrade kits are the specific threat technology being investigated by this study. They are a potential threat because they are currently being offered for export by several companies on the international market. If the proliferation market for these modular TDDs is modeled, therefore, it may provide information on the level of sophistication of mine inventories, previously purchased mines, or even an indigenous mine production capability.[112]

E. CUSTOMIZING THE TDD PROLIFERATION MARKET MODEL

The development of a threat technology market model must begin with an investigation of the underwater mine market in general. This report uses the Mine Warfare Plan (MWP) as the starting point for this investigation. The MWP is useful for several reasons. First, the goal of this research is to add to the currently existing literature on the subject, not to repackage known information. The unclassified version of the MWP provides a benchmark against which open source information gathered by this method can be compared. Second, the MWP

---

[111]Mine Warfare Plan, p. 31.

[112]A country may have an indigenous, though relatively unsophisticated mine production capability that can be upgraded with the TDD kit.

highlights those areas of mine warfare that need immediate attention, providing invaluable guidance for the selection of the threat technology. Finally the MWP is a contemporary document (published in 1992), that reflects post-Cold War thinking and incorporates the mine warfare lessons learned from Operation Desert Storm. It successfully serves as a primer on the current condition of U.S. mine warfare and its requirements for the future.

1. The Mine Market

The MWP approaches the threat posed by underwater mine proliferation from the aspect of national mine production and export activity. It states that "21 countries are known to produce mines and 13 are confirmed mine exporters." Only 16 of these mine producing countries are cited in the MWP, however. These are shown below in Table 1.

CHILE	NORTH KOREA
CHINA	RUSSIA
DENMARK	SOUTH AFRICA
FRANCE	SPAIN
GERMANY	SWEDEN
IRAQ	TAIWAN
ITALY	UNITED KINGDOM
JAPAN	YUGOSLAVIA

TABLE VIII: Mine Producing Countries(Source: Mine Warfare Plan)

It is interesting to note that 11 of the 16 nations are either allies or have a neutral foreign policy in regard to the United States. Of the others, one (Yugoslavia) no longer exists as a nation-state, two (Russia and China) have

improving relations with the United States, and another (Iraq) is currently controlled by UN sanctions and forces. At this time there is only one country, North Korea that produces mines, is hostile to the United States, and is insulated from U.S. influence.

By including non-enemies in its survey, the MWP highlights one of the unique aspects of post-Cold War threat evaluation. The national security establishment can no longer focus on potentially hostile nations exclusively but must contend with potentially hostile environments. Any actor operating in this hostile environment must be evaluated. This entails breaking traditional taboos against collecting intelligence on U.S. friends and allies.[113] Ironically, those actors who are most ardently pursuing capitalism generate the most concern in a proliferation environment dominated by financial rather than ideological motivations. U.S. allies or U.S. based firms, therefore, may contribute to this hostile environment in the future.

Export controls cannot be relied upon to counter the proliferation threat. Multilateral controls are being phased out in the COCOM countries and are weak unilateral regimes, if they exist at all, in the other producing countries. Russian Defense Ministry officials confirmed that there are no national controls on the sale of former Soviet military stockpiles. Export discretion is at the hands

[113] This can be accomplished without violating any laws or norms of international behavior by using open sources.

of "plant managers."[114] If the primary motivation behind proliferation is financial gain, then an understanding of the business aspects of proliferation is needed to counter the threat.

Proceeding from the assumption that proliferation is primarily a function of corporate not government activity, an attempt was made to determine which companies make up the mine industry. The following companies, compiled from a review of open source literature, are advertised producers of naval mines and parts or have been involved in some form of underwater mine production, including bidding for contracts, during the ten year period 1983-1993. (See Table VIII).

Compiling lists of companies, however, does not go very far toward the goal of evaluating the threat posed by the proliferation of mines and their associated technologies. It is much more helpful to know how these companies are related to one another in the context of the global underwater mine market. The list in table three includes competitors, subsidiaries, subcontractors, suppliers, as well as companies related to each other through joint ventures and co-production agreements. Defining these companies as actors, and placing them in their correct relative position in a mine proliferation market model, is the first step in the procedure to monitor proliferation.

---

[114]Interview with Dr. Vitaly Shylkov, Counselor to the Russian Ministry of Defense, at the Naval Postgraduate School, November 1993.

COMPANY	COUNTRY	COMPANY	COUNTRY
AB PRECISION (POOLE) LTD	(UK)	THIOKOL	(USA)
AEG AKTIENGESELLSCHAFT	(GER)	THOMSON SINTRA ASM	(FRA)
AEROJET TECHSYSTEMS	(USA)	THORN EMI ELECTRONICS LTD	(RUGELEY,UK)
AUSTRALIAN DEFENSE INDUSTRIES	(AUS)	VALSELLA MECCANOTECNICA	(ITA)
BAJ VICKERS	(UK)	UNDERWATER STORAGE	(UK)
BAZAN	(SPA)	WHITEHEAD MOTOFIDES	(ITA)
BEAB	(SWE)		
BODENSEEWERK GERATETECHNIK GMBH	(GER)		
BOFORS A/B	(SWE)		
BRITISH AEROSPACE AUSTRALIA	(AUS)		
BRITISH AEROSPACE PLC	(UK)		
BRITISH AEROSPACE (DYNAMICS) LTD	(UK)		
CHACONSA	(SPA)		
CHINA STATE SHIPBUILDING	(PRC)		
CONSUB EQUIPMENTOS E SERVICOS	(BRA)		
COR INC	(USA)		
DALIAN WARSHIP INST	(PRC)		
DANISH AEROTECHNOLOGYSYSTEMS A/S	(DEN)		
DEE TECHNOLOGY GROUP	(UK)		
DEWEY ELECTRONICS CORP	(USA)		
DORNIER	(GER)		
DOWTY DEFENCE AND AIR SYSTEMS LTD	(UK)		
DYNAMIT NOBEL AG	(GER)		
EQUIPOS ELECTRONICOS EESA	(SPA)		
ERICSON RADIO SYSTEMS	(UK)		
EXPAL	(SPA)		
FABRICAS Y MAESTIANZAS DE EJERTO	(CHI)		
FAUN-HAG LAUF AD PEGNITZ	(GER)		
FERRANTI - CHEADLE HEATH DIVISION	(UK)		
FFV	(SWE)		
FREQUENCY ENGINEERING LABORATORIES	(FARMINGDALE N.J.)		
GEC AVIONICS	(UK)		
GEC-MARCONI ELECTRONIX	(UK)		
GIDROPRIBOR CENTRAL RESEARCH INST	(RUSSIA)		
GOODYEAR AEROSPACE DIVISION	(AKRON, OHIO)		
GOULD	(UK)		
HITACHI ZOSEN CO LTD	(JPN)		
HONEYWELL - UNDERSEA SYSTEMS DIV	(USA)		
HUNTING ENGINEERING	(UK)		
INDUSTRIAS CARDOEN	(CHILE)		
KENG CHIEH ENTERPRISES	(TAW)		
INISEL	(SPA)		
KRUPP ATLAS ELECTRONIK GMBH	(GER)		
LAWBOROUGH CONSULTANTS	(UK)		
LOCKHEED CORP	(USA)		
LOCKLEY MANUFACTURING	(NEW CASTLE, PA)		
LORAL SYSTEMS GROUP	(USA)		
MARCONI UNDERWATER SYSTEMS	(UK)		
MESSERSCHMITT- BOLKOW BLOHM - MBB	(GER)		
MISAR SPA	(ITA)		
MITSUBISHI	(JAP)		
NEA LINDBERG A/S	(DEN)		
NORTHBEND INSTRUMENTS	(SA)		
PLESSEY - NAVAL SYSTEMS DIVISION	(UK)		
REPAIR CRAFT LTD	(UK)		
ROYAL ORDNANCE PLC	(UK)		
SA MARINE A/B	(SWE)		
SHORT BROTHERS	(UK)		
SIMA	(PERU)		
SOCIETA INDUSTRIALE CARDANA SIC	(SPA)		
SPERRY GYROSCOPES	(USA)		
TECHNICAL MANAGEMENT SERVICES	(EDINGURGH)		
TECHNOVAR	(ITA)		
TEK SEA	(SWITZERLAND)		

TABLE IX: Mine Producing Companies. (Primary Sources: Aero and Defense Markets Database, Jane's Internatnl Defense Directory 90, Jane's Underwater Weapons Systems 1993-94.)

A preliminary analysis of this data set indicates that viewing mine production solely as the activity of a nation-state produces a somewhat misleading picture of the industry. For instance, the SM G2 ground mine is considered a product of Germany, but, in fact, is a product of 13 German and Danish companies whose prime contractor, Krupp-Atlas Electronic, is a multinational corporation headquartered in Germany. Another example is "Spanish" mine production. The French company Thomson CSF, through foreign investment, owns a 49 per cent share of the Spanish company EESA[115] and therefore has considerable influence over the company's activities.

Monitoring the proliferation of the weapon system using the modeling method is somewhat easier than the stated goal of this project: monitoring the technologies. In order to prove the utility of the method at this more difficult level of analysis, a subset of the above list is selected, i.e., those companies that are involved in the proliferation of Target Detection Devices.

2. TDD Market

A summary of the logic used to determine the threat technology is displayed in Table X. Specific information that is useful in

WARFARE AREA - MINE WARFARE
SUB-AREA OF CONCERN - MINING CAPABILITY
TECHNOLOGY OF CONCERN - MINE SENSORS
THREAT TECHNOLOGY - TARGET DETECTION DEVICES

TABLE X: Investigation Logic

[115]Foxwell, p. 129.

customizing the TDD proliferation market model must now be found. The search techniques used are based on an assumption that the needed information does exist in databases and that the only obstacle to information retrieval is asking the right questions. The goal of this exercise is determining who are the actors (sources and users) and how technology proliferates within the market. Any information concerning the four major elements of the model (i.e., actors, industrial activities, corporate strategies, or distribution channels) will help customize the model. The list of questions that served as guideposts for this investigation is shown below.

QUESTIONS THAT RELATE TO HI-TECH PRODUCTS OF INTEREST
(1) How is the product referred to in the literature?
(2) Are there different names for the same item?
(3) Does it have a specific code (SIC, HCC).
(4) What is the code most closely associated with it?
(5) Is it advertised?
(6) Who makes it?
(7) Who are the foreign affiliates/subsidiaries of the producing companies? suppliers? subcontractors?
(8) What is the physical location of the plant or plants that make the product?
(9) What is the unit cost?
(10) What are its physical characteristics?
(11) How is it stored?
(12) How is it transported? Are there any special handling, packaging or shipping requirements. (HAZMAT?).
(13) Who is buying it.
(14) Is the item exported as an individual commodity?
(15) Is there any special paperwork that must be filed for the transaction?

TABLE XI: Investigation Questions

Of the companies listed in table three above, there are three that are advertised as exporters of TDD upgrade kits: Whitehead Motofides, British

Aerospace, and Dalian Shipbuilding.[116] Northbend Instruments produces a modular TDD that can be exported as a separate module.[117] Inisel produces the electronics for the MOM-90 mine including the microprocessor controlled TDD.[118] Krupp-Atlas Electronik produces the TDD for the SM-G2 ground mine.[119]

F. SUMMARY

It is impractical to monitor the proliferation patterns of every technology. Analysts must concentrate on "threat technologies," i.e., those technologies that directly challenge the superiority of existing military weapons and systems. Underwater mine upgrade kits are examples of a high technology application that enhances the military sophistication of a weapon.

Mines are a low cost, conventional deterrent that may prove decisive to the outcome of limited regional or littoral warfare. The ability to upgrade existing warstock mines to microprocessor controlled, multiple sensor, "smart weapon" systems significantly alters the calculus used to plan certain military operations.

---

[116]Jane's Underwater Weapon Systems, 1993-94.

[117]Foxwell, p. 126.

[118]"Inisel Develops New Spanish Mine," Naval Forces, p. 104, Vol. 10 No. 4, November 04, 1989.

[119]"Atlas Electronik - SM G2 Sea Ground Mine,"Maritime Defense, May 1992, pp. 126-129.

The degree to which these upgrade kits pose a threat can be evaluated by investigating the market for these Target Detection Device (TDD) upgrade kits.

Proliferation intelligence for the TDD upgrade kit focuses on the source of the devices, companies legally pursuing profitable international business opportunities. The mine industry is characterized by a limited number of suppliers, that is, it is highly concentrated. The highly concentrated nature of the industry is even more prevalent when looking at TDDs. Although many of the companies participating in the TDD market are headquartered in countries that are traditional U.S. friends and allies, every actor within the market must be evaluated without prejudice.

This case study reflects the first iteration of the investigation of the TDD market. With adequate time, financial support, and the appropriate level of interest, the technology monitoring method developed in this thesis can provide usable proliferation intelligence not only on mines but on technologies across the spectrum of warfare.

V. CONCLUSIONS

A. IMPLICATIONS

Secretary of Defense Aspin has designated the proliferation of weapons of mass destruction as one of four dangers to U.S. national security in the post Cold War world.[120] The U.S. government intends to combat this threat on a "wide variety of fronts: policy; weapons acquisition; intelligence; analytical capabilities; export controls; and international political regimes."[121]

This thesis addresses the changing nature of proliferation and focuses on the most problematic aspect of the threat: technology proliferation. Since technology is not yet fully integrated into the proliferation agenda, this technology monitoring method can compliment and strengthen the government's proliferation policy.

There are two unique aspects to this monitoring method. First, it concentrates on the commercial aspects of proliferation. Second, it relies exclusively on open sources.

---

[120]Aspin, Les, Secretary of Defense, The Bottom Up Review: Forces for a New Era, U.S. Government Printing Office, September 01, 1993.

[121]Aspin, Les, The Clinton Defense Plan, Secretary of Defense: Statement Before the Senate Armed Services Committee, April, 01, 1993.

1. Implications of Proliferation Markets

This monitoring method views technology proliferation as a systematic process. By understanding the elements of the system and how the process works, a variety of options can be designed to counter technology proliferation.

Most technology proliferation is inherently non-threatening or "benign" from a military security perspective. Threats emerge from an environment in which the proliferation of technology may be detrimental to U.S. national interests. These threatening, "malignant," markets involve some combination of three elements: an inherently threatening technology; a technology user who has hostile intentions toward the United States; or a questionable proliferation pattern (e.g., an Iranian corporation's investment in the developing free market economies of Eastern Europe.) Benign markets may become malignant if, for example, intentions of the technology user change, or a new military application for a previously non-threatening technology is developed.

The primary actors in technology markets are corporations rather than countries. Even in the case of technology procurement for national use, the proliferation occurs between state owned companies or, more frequently, companies under contract from a government. Maintaining a corporate level of analysis allows the proliferation variables associated with Multinational Corporations (MNCs), such as licensing and foreign investment, to be incorporated into the method.

A different analytical perspective must be maintained also, because threat evaluation is conducted in an "environment" rather than on a traditional "enemy." Since unrestrained capitalism poses the greatest proliferation threat, analysts must think like capitalists and learn to appreciate financial vs ideological motivations for proliferation. Any actor operating in the threat environment is evaluated regardless of their national affiliation. This may include breaking the taboo against collecting intelligence on traditional friends and allies. The end product of this method is a model that provides a visual representation of a specific technology market. Once a malignant market has been identified, the model highlights specific market vulnerabilities such as dependence on foreign suppliers, production bottlenecks, and logistic chokepoints. It also makes apparent the specific points at which leverage (i.e., diplomatic request, political suasion, economic sanction, or military force) can be applied to the market in order to stop the proliferation.

It is impossible to monitor all technologies at once. A limited number of technologies are especially threatening because they alter fundamentally the calculus used to determine the technological superiority of U.S. forces. Technologies associated with WMD are most often cited, but "threat technologies" exist across the spectrum of warfare. As used in this report, threat technologies are those associated with high-tech components that can be used to significantly enhance or upgrade the sophistication of a weapon or military system.

It is the nature of high-tech products, those that have a higher ratio of R&D expenditures to shipments, that many of their associated industries are characterized by very few producers, i.e., the industries are highly concentrated. This is clearly pointed out in a recent Wall Street Journal article entitled "Chokepoints- Computermakers Face Hidden Vulnerability: Supplier Concentration."[122]

The Japanese company *Sumitomo Chemical* suffered an explosion at its resin factory. This one factory was responsible for 65% of the resin necessary to seal computer microchips. The most interesting thing about the situation is that insiders to the industry were not aware of importance of the plant but also not surprised that these chokepoints existed. Industry is structured to be competitive, efficiency often means relying on single sources. If concentration is this severe at the industry level, it is probably more so at the product level.

Corporate actors conducting business inimical to the interests of the United States are vulnerable to different types of leverage than state actors. Domestic laws, multiple subsidiaries, and corporate image are variables unique to industry. Most corporations make many products. Pressure to change the marketing strategies for any one particular product may not be strongly opposed because of the potential negative consequences on the entire product line. The United States recently applied leverage to a Thai company that was building fall

---

[122]Hamilton, David, P., "Chokepoints - Computermakers Face a Hidden Vulnerability: Supplier Concentration," p. 1, Wall Street Journal, 27 August 1993.

out shelters in Libya. A diplomatic protest from the U.S. government to the Thai government resulted in the investigation and ultimate arrest of the Thai construction company president for violating domestic employment laws.[123]

This method is well suited to proactive, peacetime intelligence or collection during the pre-conflict stage of a crisis such as the six month prelude to the Gulf War, Operation Desert Shield. Specific information on the Iraq's French made air defense system, for example, could have been provided. A market model does not have to be completely customized to be useful. Partial models may provide the necessary data to interrupt the flow of threat technologies. The monitoring method can be triggered by other intelligence sources that indicate a benign market becoming malignant or, conversely, can be used to narrow the scope of the problem so that other intelligence assets can be brought to bear.

2. Implication of the Use of Open Sources

Commercial computerized databases are an open source, off-the-shelf resource that can be used to augment traditional assets conducting proliferation intelligence. To the extent that proliferation intelligence is economic intelligence, commercial computerized databases are uniquely optimized.

A lot of time and effort has been devoted to building and maintaining database for intelligence purposes but there has been not much emphasis on the

---

[123]Shenon, Philip, "Work by Thais in Libya Prompts a Warning by U.S.," The New York Times, 26 October 1993.

exploitation of databases produced by sources external to the national security community. The dynamism in both hardware and software technology is making databases easier to use and allowing vast amounts of information to be placed into computerized format. These advances have converged with profound geopolitical changes to make commercial computerized databases useful for solving many new problems and exploitable in ways that were never before possible.

Commercial computerized databases are a product of the information revolution. They constitute some of the first paved stretches of the National Information Superhighway, and more importantly, are part of a rapidly developing global telecommunications/information network. Other applications of this global information network and its implications for national security are topics for future research.

B. TOPICS FOR FUTURE RESEARCH

This thesis uses open sources and applies business intelligence techniques to the problems associated with technology proliferation. Unfortunately, the thesis was able only to provide an introduction. The second, third and fourth iterations of the investigation of the Target Detection Device market were not accomplished due to time constraints.

A proof of concept for this technology monitoring method is now required. It should take the form of a fully funded research project that responds to a

current technology proliferation threat. The project should include a clear means to determine the measure of effectiveness. Funding must be substantial enough to cover approximately four days of computer training in elementary through advanced database searching techniques, as well as all online and download fees associated with retrieving the information. Since it will provide the prototype for future research, allowance must be made for following and discounting "dead ends."

This project uses a mine warfare case study in order to make the point that technologies below the WMD threshold cannot be ignored. This method, however, is applicable to all technologies, military, commercial, and dual-use, across the spectrum of warfare.

VI. BIBLIOGRAPHY

Alic, John, et al, Beyond Spinoff: Military and Commercial Technologies in a Changing World, Harvard Business School Press. Boston, 1992.

Aspin, Les, The Bottom Up Review: Forces for a New Era, Office of the Secretary of Defense, September 01, 1993.

Bergsten, Fred C., "The World Economy After the Cold War," Foreign Affairs, Summer 1990.

Blanchard, et al., Reform in Eastern Europe, United Nations University, 1992,

Bradsher, Keith, "U.S. Plans More Aid to Exports", The New York Times, 30 September 1993.

Brown, Ronald H., "Toward a National Security Export Strategy," Trade Promotion Coordinating Committee Report to the U.S. Congress, September 30, 1993.

Brzoska, Michael, and Ohlson, Thomas, Arms Transfers to the Third World, 1971-1985, Oxford University Press, 1987.

Center for Non-Proliferation Studies, Inventory of International Non-Proliferation Organizations and Regimes. June 1993.

Davis, Stanley, "Organization Design," Handbook of International Business, Walter and Murray ed., John Wiley and Sons, N.Y., 1982.

Defense News, 6-12 September, 1993.

Department of Defense, Critical Technologies Plan, ES-2, 15 March, 1991.

Douglas, Susan P., and Craig, C. Samual, "Information for International Marketing Decisions," Handbook of International Business, Walter and Murray, ed., John Wiley and Sons N.Y. 1982.

Executive Office of the President, Standard Industrial Classification Manual 1987, Office of Management and Budget.

Foxwell, David, "Naval Mine Warfare: Unfunded and Underappreciated," International Defense Review, Vol 2, 1993.

Friedman, Thomas L., "Clinton's Security Aid Gives A Vision of Foreign Policy," The New York Times, 22 September 1993.

Greenhouse, Steven, "One Billion in Sales of High-Tech Items to China Blocked," The New York Times, 26 August 1993.

Hamilton, David, P., "Chokepoints- Computermakers Face a Hidden Vulnerability: Supplier Concentration," Wall Street Journal, 27 August 1993.

Hartmann, Gregory, Weapons That Wait: Mine Warfare in the U.S. Navy, Naval Institute Press, 1979.

Inman, B. R. and Burton, D. F., Jr., "Technology and U.S. National Security," Rethinking America's Security, Allison and Treverton ed., W.W. Norton and Company, New York, 1992.

Levy, Clifford J., "A Wary Reply To South Africa's Call," The New York Times, 21 October 1993.

Magee, John F., Copacino, William C., and Rosenfeld, Donald B., Modern Logistics Management: Integrating Marketing, Manufacturing and Physical Distribution, John Wiley and Sons, N.Y., 1985.

Mearsheimer, John, Conventional Deterrence, Cornell University Press, 1983.

"Naval Mine Warfare Supplement," International Defense Review, 11/1989.

Jane's Undersea Warfare 1993-94, Jane's Information Group Ltd. 1993.

Jeremiah, ADM David, "The Military and the Four Technological Revolutions," Defense Issues, Vol 8 No 5, February 16, 1993.

Meier, Gerald, M., Leading Issues in International Development, Fifth Edition, Oxford University Press, 1989.

Munro, Neil, "Pentagon Braces for New High-Technology Threats," Defense News, September 6-12, 1993.

National Academy of Engineers, National Interests in an Age of Global Technology, National Academy Press, Washington D.C. 1991.

Nelson, Richard R. and Wright, Gavin, "The Rise and Fall of American Technological Leadership: The Postwar Era in Historical Perspective," Journal of Economic Literature, Vol XXX, December, 1992.

Office of the Chief of Naval Operations, Mine Warfare Plan: Meeting the Challenges of an Uncertain World, Department of the Navy, 1992.

Porter, Michael, The Competitive Advantage of Nations, The Free Press, 1990.

Powell, Gen. Colin, National Military Strategy of the United States, 1993. U.S. Government Printing Office, Washington, D.C.

Ramirez, Anthony, "A War Within a Single Wire," The New York Times, 27 October 1993.

Richelson, Jeffry T., The U. S. Intelligence Community 2nd ed., Harper Business, 1989.

Root, Franklin, "Entering International Markets," Handbook of International Business, Walter and Murray ed., John Wiley and Sons, 1982.

Sheaffer, Radm Edward D., Office of Naval Intelligence Posture Statement, May 1993.

Shenon, Philip, "Indonesia Improves Life For Many But the Political Shadows Remain." The New York Times, 27 August 1993.

Shenon, Philip, "Work by Thais in Libya Prompts a Warning by U.S.," The New York Times, 26 October 1993.

Steele, Robert D., "Open Source Intelligence Clarifies Global Threats," Signal, September 1992.

Studemann, Admiral William, "Teaching The Giant To Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community". Unpublished paper presented at the First International Symposium on National Security and National Competitiveness: Open Source Solutions, December 1992.

Taylor, Charles R., "Global Presence and Competitiveness of the U.S. Manufactures," Conference Board, New York, 1991.

U.S. Department of Commerce, Office of Administration, Lexicon of Trade Terms, 1992.

U.S. General Accounting Office, Foreign Technology: U.S. Monitoring and Dissemination of the Results of Foreign Research, Report No. GAO/NSIAD-90-117, Government Printing Office, Washington D.C. 1990.

U.S. General Accounting Office, Foreign Technology: Federal Processes for Collection and Dissemination," Report No. GAO/NSIAD-92- Government Printing Office, Washington D.C., 1992.

Unclassified internal memorandum from Office of Naval Intelligence to National Security Affairs Department, Naval Postgraduate School, April 1993.

United States Department of the Navy, ...From the Sea: Preparing the Naval Service for the 21st Century, Government Printing Office, September 1992.

Valentine, Rep. Tim, "Critical Technology: OSTP Report," Congress, House, Committee on Science Space and Technology, Subcommittee on Technology and Competitiveness, 102nd Cong., 1st sess., 25 April 1991.

Wallerstein, Mitchell B., "Controlling Dual-Use Technologies in the New World Order," Issues In Science and Technology, pp. 70-77, Summer 1991.

Williams, Martha E., "The State of Databases Today: 1993" Gale Directory of Databases, Gale Research Inc. January 1993.

Yip, George, Total Global Strategy: Managing for Worldwide Competitive Advantage, Prentice Hall, 1992.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria VA 22304-6145	2
2.	Library, Code 052 Naval Postgraduate School Monterey CA 93943-5002	2
3.	RADM Philip A. Dur N51, The Pentagon, Room 4E566 Office of the Chief of Naval Operations Washington, D.C. 20350	1
4.	Director, Naval Intelligence (N2) The Pentagon, Room 5C600 Washington, D.C. 20350	1
5.	Mr. Paul Wallner U.S. Government Washington, D.C. 20505	1
6.	N511, The Pentagon, Room 4D563 Office of the Chief of Naval Operations Washington, D.C. 20350	1
7.	CAPT E.A. Smith, Jr, USN CNO Executive Panel (N-00K) 4401 Ford Ave. Alexandria, VA 22302	1
8.	CAPT R. Perkins, USN Office of Naval Intelligence (ONI-2) 4301 Suitland Road Washington, D.C. 20395-5000	1

9. Mr. Robert D. Steele — 1
1914 Autumn Chase Court
Falls Church, VA 22043-1753

10. Dr. Thomas C. Bruneau — 1
Chairman, National Security Affairs (NS/Bn)
Naval Postgraduate School
Monterey, CA 93943

11. Dr. Robert E. Looney — 1
National Security Affairs
Naval Postgraduate School
Monterey, CA 93943

12. Dr. Edward J. Laurance — 1
International Policy Studies
Monterey Institute of International Studies
425 Van Buren Street
Monterey, CA 93940

13. Mr. Charles O. Green — 1
1613 Eva Ave
Joppa, MD 21085